GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas

INSTITUTO NACIONAL DE **TECNOLOGÍAS** DE LA **COMUNICACIÓN**

Edición: Septiembre 2012

El "Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas" ha sido elaborado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO):

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Eduardo Álvarez Alonso

Laura García Pérez

Susana de la Fuente Rodríguez

INTECO quiere señalar el apoyo técnico en la realización de la investigación de:

MADISON®
MARKET RESEARCH

ÍNDICE

PUNTOS CLAVE 5

I Protección de la empresa española 5

II Incidentes de seguridad en la empresa española 7

III E-confianza 8

IV Recomendaciones 8

1 INTRODUCCIÓN Y OBJETIVOS 10

1.1 Presentación 10

1.2 Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas 12

2 METODOLOGÍA 14

2.1 Fase 1: análisis documental 14

2.2 Fase 2: encuesta a empresas 14

2.3 Fase 3: entrevistas en profundidad 20

2.4 Fase 4: grupo de trabajo final con expertos cualificados 22

3 HERRAMIENTAS TÉCNICAS Y PERSONAL DE SEGURIDAD 24

3.1 Herramientas de seguridad en la empresa española: implantación y motivación 25

3.2 Seguridad en dispositivos móviles y comunicaciones inalámbricas 29

3.3 Personal dedicado a la seguridad de la información 33

3.4 Estrategia corporativa en seguridad e implicación de la dirección 36

4 BUENAS PRÁCTICAS DE SEGURIDAD 38

4.1 Copias de seguridad 38

4.2 Actualización de programas y sistemas 43

4.3 Medidas de control de acceso a equipos y documentos 44

4.4 Buenas prácticas en dispositivos móviles 45

4.5 Buenas prácticas para los empleados 46

5 PLANES Y POLÍTICAS DE SEGURIDAD 50

5.1 Percepción de la empresa sobre planes y políticas de seguridad 50

5.2 Análisis del conocimiento sobre medidas o Planes de Continuidad de Negocio 52

5.3 Situación de seguridad de la empresa española desde el punto de vista de la continuidad de negocio 54

6 INCIDENTES DE SEGURIDAD EN LA EMPRESA: INCIDENCIA, IMPACTO Y RESPUESTA 66

6.1 Percepción de las empresas sobre la evolución general de los incidentes de la seguridad 66

6.2 Percepción de las empresas sobre sus incidentes de seguridad 67

6.3 Impacto y consecuencias de los incidentes 74

6.4 Respuesta de las empresas frente a los incidentes de seguridad 77

7 E-CONFIANZA DE LA PEQUEÑA Y MEDIANA EMPRESA ESPAÑOLA 81

7.1 E-confianza en la Sociedad de la Información 85

7.2 Frenos al desarrollo de la Sociedad de la Información 94

8 PERFILES DE SEGURIDAD Y CONTINUIDAD DE NEGOCIO EN LA EMPRESA 96

8.1 Perfiles relacionados con la seguridad de la información y e-confianza 96

8.2 Perfiles relacionados con la continuidad de negocio 101

9 CONCLUSIONES 106

9.1 Puntos débiles 106

9.2 Puntos fuertes 107

9.3 Amenazas 108

9.4 Oportunidades 109

10 RECOMENDACIONES DE ACTUACIÓN 111

10.1 Recomendaciones para la micro, pequeña y mediana empresa 111

10.2 Recomendaciones dirigidas a la industria de seguridad 114

10.3 Recomendaciones dirigidas a la Administración Pública 116

ÍNDICE DE GRÁFICOS 118

ÍNDICE DE TABLAS 122

ANEXO I: BIBLIOGRAFÍA 123

PUNTOS CLAVE

El *Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas* realiza un diagnóstico de la percepción sobre el nivel de preparación ante los riesgos de seguridad y la adopción de estrategias de continuidad de negocio por parte de las pequeñas y medianas empresas españolas que utilizan Internet como parte de su negocio en 2012.

Para llevar a cabo la investigación, se ha desarrollado una metodología que comprende: encuestas a una muestra representativa de empresas españolas de menos de 250 empleados repartidas por todo el territorio nacional y entrevistas en profundidad a responsables en seguridad de la información de las empresas. Asimismo, Los resultados de la encuesta han sido sometidos a la consideración de un grupo de expertos, cuyas aportaciones han sido esenciales para la comprensión de la situación de la empresa española.

A continuación se exponen los puntos clave del estudio.

I PROTECCIÓN DE LA EMPRESA ESPAÑOLA

En general, el colectivo de pequeñas y medianas empresas españolas declaran un notable grado de implantación de las herramientas de seguridad básicas, normalmente incluidas en soluciones paquetizadas. Aunque estas perciben que la seguridad ha mejorado en el último año, existe un margen de mejora en cuanto a la incorporación de medidas más allá de las tradicionales, que abarquen no sólo el componente técnico, sino también el organizativo y estratégico.

- Antivirus y cortafuegos son herramientas que presentan una amplia penetración en las organizaciones (un 96,1% y un 75,4%, respectivamente). Por detrás de estas se sitúan medidas que implican la participación del usuario o proporcionan funcionalidades específicas.

- Los dispositivos móviles, cada vez con más peso en las empresas, están menos protegidos que los equipos informáticos. Así, un 96,1% de los ordenadores dispone de antivirus, porcentaje que desciende al 21,8% en terminales móviles.

- Respecto a la protección de la red inalámbrica wifi, es necesario extender la incorporación de los estándares WPA/WPA2. En el presente informe, WPA/WPA2 y WEP (estándar inseguro) son declarados en la misma proporción (un 27,4%).

- Un 56,3% de las empresas españolas afirman disponer de recursos humanos destinados a la seguridad de la información (un 21,0 % mediante personal interno y un 35,3% a través de una empresa externa).

- De forma general, las empresas opinan que la seguridad de la información ha evolucionado favorablemente en el último año (un 70,2% indican que esta es igual o superior a la de 2011). Un factor que influye en la evolución es el amplio compromiso de la dirección por la protección de la información (un 72,3% lo consideran muy o bastante importante).

Junto con las herramientas, las organizaciones adoptan en gran medida hábitos de protección como las copias de seguridad o la actualización del sistema operativo y programas. El esfuerzo debe dirigirse a la concienciación y formación en la adecuada utilización de las mismas.

- En base a las declaraciones de las empresas, es reseñable la adopción mayoritaria de prácticas como la realización de copias de seguridad (un 88,2%), la actualización del sistema operativo y los programas (81,9%) y las medidas de control de acceso a equipos y documentos (69,1%).

- Estas prácticas deben acompañarse de las actuaciones necesarias que garanticen la disponibilidad, integridad y confidencialidad de la información. Por ejemplo, estableciendo adecuadamente la frecuencia de realización, el procedimiento, la ubicación, etc.

- Por el contrario, las pymes demuestran estar menos concienciadas por la protección de las tecnologías móviles y sólo un 11,7% dispone de políticas de uso seguro para los usuarios de dichos dispositivos.

- Asimismo, los hábitos prudentes dirigidos a los empleados son más minoritarios, como la limitación de acceso a Internet (21,3%), la instalación de programas a través de un responsable (45,3%) o la formación en seguridad para los trabajadores (27,3%).

La adopción de planes y políticas de seguridad que permitan asegurar la disponibilidad, integridad y confidencialidad de la información es todavía una asignatura pendiente para una gran parte de la empresa española. Tanto por el desconocimiento de lo que conlleva disponer de una estrategia de continuidad de negocio, como de la falta de consideración de estas estrategias como inversiones que permitan la continuidad de las operaciones en caso de desastre.

- Las pequeñas y medianas empresas creen realizar auditorías de seguridad y disponer de certificaciones en Sistemas de Gestión de la Seguridad de la Información (SGSI) en mayor medida que lo que afirman los datos oficiales. Ambos factores son indicadores de la apuesta de la empresa por una seguridad planificada, por lo que es necesario un mayor esfuerzo de sensibilización para salvar ese salto en la percepción.

- También se observa una oportunidad de mejora respecto a los Planes de Continuidad de Negocio. Cuatro de cada diez empresas encuestadas conoce el significado de estos planes, aunque esta proporción es inferior en cuanto a la disposición de alguna estrategia o procedimiento en caso de situaciones de crisis o desastre, bien refiriéndose a un estrategia global (15,3%), bien relativo a mecanismos para la recuperación exclusivamente del entorno tecnológico que soporta las operaciones de negocio (15,5%).

- Por último, el Plan de Continuidad de Negocio exige el seguimiento y mejora continua de los procesos. Un 31,9% de las empresas con PCN habilita mecanismos para comprobar su eficacia, entre los destaca la realización de pruebas periódicas (42,3%).

II INCIDENTES DE SEGURIDAD EN LA EMPRESA ESPAÑOLA

A juicio de las empresas, los incidentes de seguridad más frecuentes siguen siendo el malware y el spam en el caso de los ordenadores, mientras que en los dispositivos móviles son el robo y la pérdida de los mismos. Los sucesos con más probabilidad de poner en riesgo la continuidad del negocio son aquellos relativos al funcionamiento incorrecto de la infraestructura informática.

- Un 73,9% de las empresas afirma no haber sufrido un incidente de seguridad en el último año, frente a un 26,1% que sí son conscientes de esta circunstancia. Disponer de personal interno de seguridad tiene una relación directa con la mayor percepción de incidencias: el porcentaje de víctimas aumenta hasta el 46,4% entre las que cuentan con estos profesionales.

- La infección por malware (14,7%) y la recepción de correo electrónico no deseado o spam (11,9%) son las incidencias declaradas en mayor medida.

- En el caso de los dispositivos móviles, el 77,0% señalan no haber tenido ningún percance de seguridad en sus terminales durante el último año. La sustracción y la pérdida del terminal (7,2% y 7,1% respectivamente) son los sucesos más frecuentes.

- Los incidentes pueden, en ocasiones, provocar la interrupción de las operaciones de negocio. Así, en el último año el principal percance declarado es la caída o avería de los sistemas de soporte (un 15,2%), seguido de la caída de los sistemas o aplicaciones informáticas (11,3%) y la falta de servicio o suministro por parte de los proveedores (11,2%).

Tras un incidente, las empresas identifican las consecuencias más visibles, pero son menos conscientes de las consecuencias de carácter técnico. Frente a estos sucesos, las reacciones todavía son tímidas, centradas en la incorporación de nuevas herramientas y medidas de seguridad.

- Entre las empresas que declaran haber sufrido impactos negativos en su operativa, imagen o economía a consecuencia de un incidente de seguridad, los señalados en mayor medida son los que afectan al tiempo y la productividad y los que implican una parada de las operaciones.

- Un 54,4% de las organizaciones no realiza ninguna modificación después del percance, mientras que un 38,5% adopta una actitud proactiva incorporando herramientas o medidas de seguridad. Sin embargo, no existe una apuesta clara por actuaciones a nivel organizativo o estratégico.

- Los encargados de resolver los incidentes son los técnicos internos de las empresas (según declara un 48,5%), aunque destaca la proporción de organizaciones que dicen apoyarse en un servicio externo, bien para asesorar al personal de la empresa (un 7,4%), bien para resolver directamente el incidente (un 33,5%).

III E-CONFIANZA

Servicios como la banca electrónica, la e-Administración o el negocio electrónico (firma y factura electrónica) contribuyen al avance de la e-confianza en la Sociedad de la Información.

- Banca electrónica y medios de pago online (69,8%), página web empresarial (55,5%) y e-Administración (51,9%) son los servicios de Internet más extendidos en el colectivo empresarial española. Es necesario realizar un esfuerzo por promover la utilización de aquellos menos presentes, como redes sociales (26,8%%), factura electrónica (20,3%), e-contratación (17,7%) y venta online (14,5%).

- A pesar de las diferencias en el uso, destaca el alto nivel de confianza que, según las empresas, les transmiten la mayoría de los servicios. Así ocurre con la e-Administración (87,0%), la utilización de la banca electrónica y los medios de pago online (86,1%) o el negocio electrónico (83,9%). Las redes sociales son las que menos confianza generan (45,9%).

- La falta de necesidad y la falta de interés son los motivos más alegados para la no incorporación de nuevos servicios.

IV RECOMENDACIONES

Las recomendaciones que se exponen en el informe están dirigidas a las empresas, a la industria de seguridad de la información y a la Administración Pública.

Recomendaciones para las pymes

- Avanzar en la sensibilización de las empresas sobre los riesgos de seguridad de la información, incidiendo en la formación y el reciclaje internos.

- Acudir a profesionales externos que solventen la falta de recursos internos sin renunciar a la seguridad.

- Utilizar correctamente las herramientas y medidas de seguridad. Muchas empresas no disponen de los conocimientos suficientes para adaptar correctamente las soluciones a su caso concreto.

- Fomentar la incorporación de buenas prácticas para los miembros de la organización.

- Adoptar estrategias de continuidad de negocio para asegurar la resistencia de la organización ante cualquier suceso que pueda poner en peligro su supervivencia.

- Establecer criterios de seguridad en las relaciones con los proveedores.

- Mantenerse actualizados de las novedades en materia de riesgos de seguridad y medidas de protección.

Recomendaciones para la industria de seguridad

- Adecuar la oferta de productos y soluciones de seguridad a la realidad de la empresa española.
- Desplegar actuaciones que ayuden a complementar la seguridad en la empresa desde la concienciación y la formación.
- Promover la profesionalización de las empresas del canal de distribución de soluciones de seguridad.
- Colaborar estrechamente con las Administraciones Públicas.

Recomendaciones para las Administraciones Públicas

- Asesorar al empresario para que incorpore competencias de seguridad de la información.
- Desplegar acciones de sensibilización basados en los beneficios del uso de servicios TIC y la seguridad proactiva.
- Promover el desarrollo de estrategias empresariales basadas en estándares.
- Desplegar acciones informativas y formativas para el personal de las empresas.
- Estudiar el estado de la seguridad de la información y la continuidad de negocio en las empresas españolas.
- Realizar acciones específicas para las empresas de servicios de tecnologías de la información (TI).

1 INTRODUCCIÓN Y OBJETIVOS

1.1 PRESENTACIÓN

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las administraciones públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

- **Seguridad tecnológica:** INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y, por supuesto, que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT), con su Catálogo de Empresas y Soluciones de Seguridad TIC, y la Oficina de Seguridad del Internauta (OSI), de los que se benefician ciudadanos, pymes, administraciones públicas y el sector tecnológico.

- **Accesibilidad:** INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus usuarios. Y que faciliten la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. En particular, INTECO dispone de amplia experiencia en el desarrollo de proyectos en el ámbito de la accesibilidad para la televisión digital, así como de aquellos orientados a garantizar los derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, reconocidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

- **Calidad TIC**: INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software, a través del Laboratorio Nacional de Calidad del Software.

- **Formación**: la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

Es uno de los objetivos del Instituto describir de manera detallada y sistemática el nivel de seguridad, privacidad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la seguridad de la información, la privacidad y la e-confianza.

INTECO ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad y privacidad, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad y privacidad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.

- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.

- Impulso de proyectos de investigación en materia de seguridad TIC.

- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.

- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

1.2 ESTUDIO SOBRE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO EN LAS EMPRESAS ESPAÑOLAS

1.2.1 Contexto y oportunidad del estudio

Las microempresas y las pequeñas y medianas empresas son el motor de la economía europea. Constituyen una fuente fundamental de puestos de trabajo, generan espíritu empresarial e innovación en la UE y, por ello, son vitales para promover la competitividad y el empleo. Este colectivo está constituido por organizaciones que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros.

Los datos del Instituto Nacional de Estadística (INE)[1] dibujan un mapa de 3.267.521 empresas en España, de las cuales 3.245.579 tienen menos de 199 asalariados. Más del 99% del tejido empresarial español está constituido por organizaciones que encajan en la definición de microempresas, pequeñas y medianas empresas, de acuerdo con lo dispuesto por la Comisión Europea[2].

En España, este colectivo tiene una importancia estratégica en el marco del desarrollo económico del país, puesto que el tejido empresarial español está constituido en más de un 99% por pequeñas empresas y más de un 95% tienen menos de 10 asalariados.

Las Tecnologías de la Información y las Comunicaciones (TIC) desempeñan un papel dinamizador de la competitividad de la economía a nivel global e impulsan la innovación, la creatividad y la eficiencia en las organizaciones.

Ello justifica la necesidad de disponer de un diagnóstico real y riguroso de la situación de seguridad TIC en la pequeña y mediana empresa española, como paso previo a la implementación de políticas de fomento de la securización para las empresas. La vocación de INTECO hacia este colectivo le ha llevado a realizar en el pasado, a través de su Observatorio de la Seguridad de la Información, proyectos de investigación similares en las materias planteadas (seguridad de la información y continuidad de negocio). Así, en 2010 se publicó el *Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas*[3] y el *Estudio sobre el estado de la pyme española ante los riesgos y la implantación de Planes de Continuidad de Negocio*[4], fruto de sus resultados, en 2009 se editó la *Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio*[5].

---

[1] Directorio Central de Empresas (DIRCE), datos de 1 de enero de 2011. Consulta del directorio disponible en: http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t37/p201/&file=inebase.

[2] Comisión Europea (2006) *La nueva definición de PYME*. Publicaciones de empresa e industria. Disponible en: http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_es.pdf

[3] INTECO (2010). *Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas.* Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_seguridad_microempresas

[4] INTECO (2010). *Estudio sobre el estado de la pyme española ante los riesgos y la implantación de Planes de Continuidad de Negocio.* Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_pymes_continuidad_negocio

[5] INTECO (2010). *Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/guias/guia_continuidad

Por ello, el ***Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*** garantiza la continuidad de estos estudios anteriores, recogiendo la situación actual en estos ámbitos. Por otro lado, para aprovechar el potencial práctico y operativo de la información recogida, el desarrollo de esta investigación debe generar una serie de indicadores con vocación de permanencia y continuidad más allá del marco temporal del proyecto.

1.2.2 Objetivo general

El objetivo general del proyecto es la obtención de un diagnóstico riguroso sobre el nivel de preparación ante los riesgos de seguridad y la adopción de estrategias de continuidad de negocio en las pequeñas y medianas empresas españolas que utilizan Internet como parte de su negocio.

1.2.3 Objetivos específicos

El objetivo general apuntado se desglosa, a su vez, en una serie de objetivos específicos:

- Disponer de indicadores que permitan conocer cuál es la situación actual en materia de seguridad y continuidad de negocio en las empresas españolas.

- Identificar los principales incidentes que afectan a los sistemas de información e incluso, provocar la paralización de las actividades de negocio, estudiando las principales consecuencias derivadas y las reacciones adoptadas desde las organizaciones.

- Identificar patrones o perfiles de comportamiento en las empresas en cuanto a implementación de la cultura de seguridad y continuidad de negocio.

- Analizar el nivel de uso y confianza en los diferentes servicios de la Sociedad de la Información presentes en las pequeñas y medianas empresas, profundizando en los motivos que implican una menor o nula utilización de los mismos.

- Aportar una serie de conclusiones en base a los principales resultados obtenidos. Estas conclusiones permiten, a su vez, proporcionar diferentes recomendaciones a los poderes públicos, a la industria proveedora de bienes y servicios de seguridad, y a las propias empresas en el sentido de concienciar sobre la importancia de elevar el nivel de seguridad y continuidad de negocio en la estrategia empresarial española.

2 METODOLOGÍA

Para la realización de este estudio se ha utilizado una combinación de técnicas de análisis cualitativo y cuantitativo, estructurando el proyecto en varias fases:

- **Fase 1**: Búsqueda y análisis documental (fuentes primarias y secundarias).
- **Fase 2**: Encuesta a responsables en seguridad de la información y continuidad de negocio en las pymes.
- **Fase 3:** Entrevistas en profundidad a responsables de seguridad de la información y continuidad de negocio en las empresas, seleccionados en función de la caracterización de las pymes en diferentes perfiles de comportamiento.
- **Fase 4**: Grupo de expertos en seguridad de la información y continuidad de negocio pertenecientes a diferentes ámbitos.

2.1 FASE 1: ANÁLISIS DOCUMENTAL

El objetivo de esta primera fase ha sido recoger información sobre la situación actual y evolución del grado de securización de la pequeña y mediana empresa española y la posición respecto a la adopción de planes de continuidad de negocio.

Como fuentes documentales se han utilizado los diferentes informes realizados por INTECO en las materias objeto del presente estudio. Asimismo, se han tenido en cuenta informes, *white papers*, estudios y notas de prensa de múltiples fuentes nacionales e internacionales como herramientas para llevar a cabo la investigación documental. La procedencia de estas fuentes abarca organismos oficiales (Eurostat, INE, ONSTI, etc.), empresas relacionadas con las tecnologías de la información y las comunicaciones (Everis, Deloitte, PricewaterhouseCoopers) e industria de la seguridad de la información (Panda Security o Kaspersky), entre otras.

En el ANEXO I: BIBLIOGRAFÍA se pueden encontrar las fuentes de los documentos clave utilizados. De la misma manera, se citan como pie de gráficos y tablas las fuentes utilizadas para la muestra de los datos en cada caso.

2.2 FASE 2: ENCUESTA A EMPRESAS

Para analizar la percepción de la situación en las pequeñas y medianas empresa española en cuanto a la seguridad y continuidad de negocio se ha realizado una fase de encuesta. La complejidad de dicha encuesta ha propiciado la división del cuestionario en dos partes, a saber:

- **Parte A: seguridad de la información y e-confianza.**
- **Parte B: continuidad de negocio.**

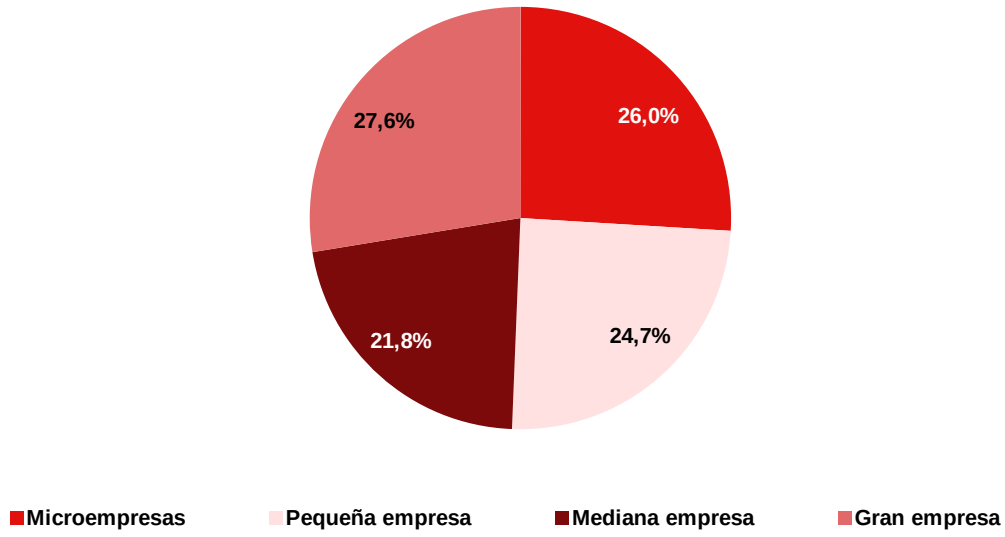
En total han participado 1.424 empresas, de las cuales 1.144 han respondido a la parte A de la encuesta (seguridad y e-confianza) y 1.109 han respondido a la parte B (continuidad de negocio).

2.2.1 Universo del estudio y sujeto de opinión

El universo objeto de estudio se compone de las pequeñas y medianas empresas españolas con al menos un ordenador conectado a Internet, estratificado en base al número de empleados y sector de actividad.

Como primera aproximación, la pequeña y mediana empresa española aglutina a gran parte del tejido empresarial español (99%), contribuyendo en gran medida a la generación de riqueza económica. Así, en el siguiente gráfico se muestra la distribución de la masa laboral en España, en base a los datos de la Encuesta de Coyuntura Laboral del INE[6]. El colectivo analizado ocupa un lugar destacado en la distribución de la masa laboral: el 72,4% de los trabajadores pertenecen a micro, pequeñas y medianas empresas, mientas que las empresas de mayor tamaño emplean al 27,6% de este colectivo.

Gráfico 1: Distribución de la masa laboral de empleados en España (%)



Fuente: Encuesta de Coyuntura Laboral - Tercer trimestre 2011

De cara a la delimitación del universo del estudio, se han tenido en cuenta los siguientes aspectos:

- Se incluye bajo la denominación de pequeña y mediana empresa a profesionales liberales y empresas de hasta 250 trabajadores, en base a la clasificación establecida por la Comunidad Europea.
- La delimitación por sector de actividad se ha realizado utilizando la clasificación nacional de actividades empresariales (CNAE) en su versión de 2009, con 6 categorías resultantes.
- Se ha realizado una segmentación propia agrupando las comunidades autónomas por zonas geográficas, obteniendo 6 divisiones.

[6] Fuente: INE (2012) Encuesta de Coyuntura Laboral - Tercer trimestre 2011. Disponible en: http://www.larioja.org/upload/documents/699790_ECL_3T11.pdf

- Los datos de empresas con conexión a Internet se han extraído de la *Encuesta de uso de TIC y Comercio Electrónico (CE) en las empresas 2010-2011* del Instituto Nacional de Estadística (INE), que proporciona las siguientes cifras a 1 de enero de 2011: 64,1% de conexión a Internet en microempresas de menos de 10 empleados, 97,0% en pequeñas empresas de 10 a 49, y el 99,4% en medianas empresas de 50 a 250 empleados.

Tabla 1: Universo del estudio

Número de empleados	Total empresas[7]	Total empresas con conexión a Internet[8]	%
Microempresas *(menos de 10 empleados)*	3.094.721	1.983.716	93,1%
Pequeñas empresas *(10-49 empleados)*	130.994	127.064	6,0%
Medianas empresas *(50-249 empleados)*	19.864	19.745	0,9%
Total	**3.245.579**	**2.130.525**	**100%**
Sector de actividad	**Total empresas**	**Total empresas con conexión a Internet**	**%**
Industria y construcción	706.643	s/d[9]	21,8%
Comercio y hostelería	1.068.649	s/d	32,9%
Transporte	216.802	s/d	6,7%
Nuevas Tecnologías	60.032	s/d	1,8%
Servicios empresariales	739.664	s/d	22,8%
Otros servicios	453.789	s/d	14,0%
Total	**3.245.579**	**2.130.525**	**100%**
Zona geográfica[10]	**Total empresas**	**Total empresas con conexión a Internet**	**%**
Zona Sur	631.586	s/d	19,5%
Zona Centro	452.184	s/d	13,9%
Cataluña	600.698	s/d	18,5%
Zona Este	526.669	s/d	16,2%
Zona Norte	534.352	s/d	16,5%
Comunidad de Madrid	500.090	s/d	15,4%
Total	**3.245.579**	**2.130.525**	**100%**

Fuente: Directorio Central de Empresas. Instituto Nacional de Estadística (INE). 2011

[7] A los efectos de cálculo de la muestra se han utilizado los datos del Directorio Central de Empresas del Instituto Nacional de Estadísticas (INE), que establece el límite del intervalo en 200 empleados. Esto no implica desviaciones significativas en el diseño muestral.

[8] Encuesta de uso de TIC y Comercio Electrónico (CE) en las empresas 2010-2011 del Instituto Nacional de Estadística (INE):
Datos para empresas de menos de 10 empleados disponibles en: http://www.ine.es/jaxi/tabla.do?path=/t09/e02/a2010-2011/l0/&file=01004.px&type=pcaxis&L=0
Datos para empresas de 10-49 y de 50-249 empleados disponibles en:
http://www.ine.es/jaxi/tabla.do?path=/t09/e02/a2010-2011/l0/&file=01002.px&type=pcaxis&L=0

[9] s/d: Sin datos

[10] **Zona Sur**: Andalucía, Ceuta, Melilla y Canarias; **Zona Centro**: Aragón, Castilla y León, Castilla-La Mancha, Extremadura; **Zona Este**: Comunidad Valenciana, Islas Baleares, Murcia; **Zona Norte**: Galicia, Asturias, Cantabria, País Vasco, Rioja, Navarra.

El estudio profundiza en la medida de lo posible, en los datos segmentados por tamaño de empresa y por ámbito sectorial.

La unidad informante de la encuesta ha sido la persona responsable de la seguridad de la información de la empresa o, en su defecto, el responsable de informática. En caso de ausencia de las dos figuras anteriores, el sujeto de opinión ha sido el responsable de la empresa.

2.2.2 Tamaño y distribución muestral

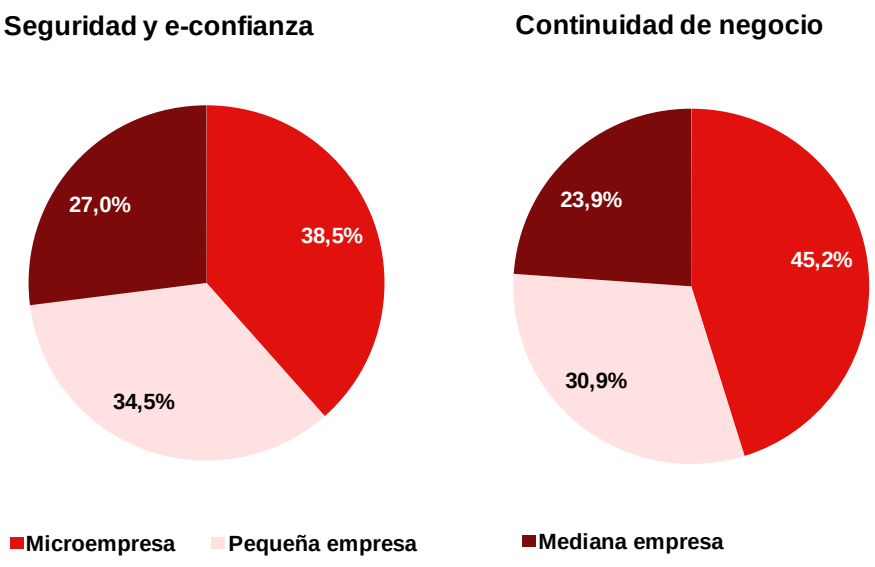
El tamaño muestral de la parte de seguridad y e-confianza de la encuesta es de 1.144 empresas y de la parte de continuidad de negocio es de 1.109, repartidas por todo el territorio nacional.

Dicha muestra se ha distribuido por estratos utilizando una solución de compromiso entre afijación uniforme y proporcional, según los datos de empresas recogidos en el Directorio Central de Empresas, del Instituto Nacional de Estadística referidos a 2011.

Para realizar el muestreo se han tenido en cuenta tres variables de estratificación: tamaño de la empresa (número de empleados), sector de actividad y zona geográfica.

En el siguiente gráfico se muestra la distribución por tamaño de la población objeto de estudio para cada una de las dos partes de la encuesta.

Gráfico 2: Distribución de las muestras por tamaño de la empresa (%)



Base: Seguridad y e-confianza (n=1.144); Continuidad de negocio (n=1.109) *Fuente: INTECO*

En ambos casos, esta distribución presenta diferencias estructurales respecto a la población real. Esto es así porque la afijación de la muestra por estratos se realizó de manera no proporcional, con el objeto de asegurar la representatividad de determinados estratos.

Por tanto, es necesario aplicar un factor de ponderación que permita guardar la proporcionalidad de cada uno de los estratos de la muestra respecto de la población real objeto de estudio. Es decir, el factor de ponderación cambia los pesos de los distintos estratos muestrales para que éstos se ajusten a los poblacionales.

En este caso, la aplicación del factor de ponderación ha supuesto asignar más peso a las respuestas aportadas por las microempresas, y menos a las pequeñas y medianas empresas, ya que dentro del conjunto poblacional existe esta diferencia entre el número de organizaciones de cada tipo. Igualmente se ha incrementado el peso de las organizaciones pertenecientes a las actividades y de las zonas geográficas cuya representatividad efectiva en el conjunto de la población es mayor que la existente en la muestra.

Por tanto, esta ponderación se ha llevado a cabo en función de las siguientes variables: tamaño de la empresa (número de empleados) y sector de actividad y zona geográfica.

Ilustración 1: Factor de ponderación

$$\left(\frac{\left(\frac{N_i}{N_t}\right)}{\left(\frac{n_i}{n_t}\right)}\right)$$

Ni= número de empresas que hay en cada estrato

Nt= número de empresas que hay en la población de referencia

ni= número de empresas que hay en cada estrato de la muestra

nt= número total de empresas que componen la muestra

Fuente: ONTSI[11]

Los datos poblacionales para la elaboración de este ponderador han sido obtenidos a partir de la información publicada por el Instituto Nacional de Estadística (INE) a través del Directorio Central de Empresas (DIRCE).

A lo largo del estudio, se describe al pie de cada gráfico la base de cálculo. Apréciese que, en estos casos, se recogen los datos reales de la muestra, sin aplicar ningún factor de ponderación, con objeto de proporcionar una visión más realista del análisis.

2.2.3 Error muestral

El error para la muestra que ha respondido a la parte de seguridad y e-confianza (n=1.144) y en la parte de continuidad de negocio (n=1.109) es en ambos casos de ± 2,9%, calculado para un nivel de confianza del 95,5%, y siendo p=q=0,50.

A pesar de que el error muestral es el indicado, el diferente peso de las empresas en función de su tamaño obliga a detallar los errores muestrales para cada uno de estos grupos, como se indica en la siguiente tabla:

[11] El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) es un órgano adscrito a Red.es cuyo principal objetivo es el estudio y análisis de la Sociedad de la Información en España.

Tabla 2: Error muestral[12]

Número de empleados	Seguridad y e-confianza		Continuidad de Negocio	
	Muestra	Error (%)	Muestra	Error (%)
Microempresa	440	±4,7%	501	±4,4%
Pequeña empresa	395	±4,9%	343	±5,3%
Mediana empresa	309	±5,5%	265	±6,0%
Total	**1.144**	**±2,9%**	**1.109**	**±2,9%**
Sector de actividad	**Seguridad y e-confianza**		**Continuidad de Negocio**	
	Muestra	**Error (%)**	**Muestra**	**Error (%)**
Industria y construcción	215	±6,7%	209	±6,8%
Comercio y hostelería	186	±7,2%	172	±7,5%
Transporte	170	±7,5%	147	±8,1%
Nuevas Tecnologías	160	±7,7%	153	±7,9%
Servicios empresariales	202	±6,9%	202	±6,9%
Otros servicios	211	±6,7%	226	±6,5%
Total	**1.144**	**±2,9%**	**1.109**	**±2,9%**
Zona geográfica	**Seguridad y e-confianza**		**Continuidad de Negocio**	
	Muestra	**Error (%)**	**Muestra**	**Error (%)**
Zona Sur	180	±7,3%	184	±7,2%
Zona Centro	179	±7,3%	172	±7,5%
Cataluña	208	±6,8%	188	±7,1%
Zona Este	206	±6,8%	188	±7,1%
Zona Norte	193	±7,1%	201	±6,9%
Comunidad de Madrid	178	±7,3%	176	±7,4%
Total	**1.144**	**±2,9%**	**1.109**	**±2,9%**

Fuente: INTECO

Estos reducidos márgenes de error aportan fiabilidad a la hora de extraer conclusiones respecto al conjunto del tejido empresarial español.

2.2.4 Realización del trabajo de campo

El trabajo de campo se ha realizado en dos momentos diferentes: la parte A (seguridad de la información y e-confianza) se ha realizado entre el 12 de diciembre de 2011 y el 13 de enero de 2012 y la parte B (continuidad de negocio) entre el 23 de enero de 2012 y el 10 de febrero de 2012.

De forma general, se ha empleado la técnica CATI (*Computer Assisted Telephone Interviewing*), complementada por CAWI (*Computer Aided Web Interviewing*).

[12] En el cálculo del error estadístico se ha considerado un universo infinito.

2.2.5 Tratamiento y análisis estadístico de los datos

A partir de la información recogida en la encuesta, se ha aplicado un plan de explotación estadística que ha permitido dar respuesta a los objetivos definidos.

El primer paso para el análisis consiste en la tabulación básica, que ofrece información general de la encuesta y permite medir la calidad de los datos. Tras analizar los listados de frecuencias, se ha procedido al diseño del protocolo de explotación de los datos y plan de tablas estadísticas y gráficos a obtener. Este proceso se ha llevado a cabo con el programa SPSS, a partir del protocolo de explotación. Se han aplicado las siguientes técnicas estadísticas y de análisis:

- **Técnicas estadísticas descriptivas** o distribución de frecuencias relativas de todas las variables categóricas del cuestionario y obtención de medias para las variables numéricas.

- **Test de inferencia estadística o test estadísticos de significación** para conocer si existen diferencias estadísticamente significativas entre las distintas categorías de una variable.

- **Análisis multivariantes** que permiten una interpretación más profunda de los datos y aportan valor añadido al estudio. En este sentido, se han realizado **dos análisis *clúster***, que consisten en clasificar una población amplia, compuesta por el total de población estudiada (pymes) en un pequeño número de grupos, mutuamente excluyentes y exhaustivos, basándose en las semejanzas de perfiles existentes entre los diferentes elementos componentes de dicha población respecto a un aspecto concreto, en este caso la seguridad de la información (primer análisis) y la continuidad de negocio (segundo).

2.3 FASE 3: ENTREVISTAS EN PROFUNDIDAD

El propósito de esta fase identificar experiencias particulares en la securización y el establecimiento de estrategias de continuidad de negocio en las empresas, extraer patrones de comportamiento y necesidades de actuación para la mejora y el desarrollo de las materias objeto de la investigación en la empresa española. Para ello, se han realizado diez entrevistas en profundidad a responsables de seguridad pertenecientes a organizaciones participantes en la encuesta, cinco relativas a seguridad de la información en la empresa, y cinco sobre continuidad de negocio. Las entrevistas han tenido lugar entre los meses de febrero y marzo de 2012.

La identificación de cada uno de los participantes en la fase de entrevistas en profundidad se ha hecho con el objetivo de cubrir la heterogénea realidad del tejido empresarial. Los criterios tenidos en cuenta para realizar la selección se han basado en las características que definen los perfiles detectados a partir de los análisis clúster, que son analizados en detalle en el capítulo 8.

- **Seguridad de la Información:** empresas “protegidas”, “precavidas”, “despreocupadas” e “imprudentes”.

- **Continuidad de Negocio:** empresas “”, “preparadas”, “desprevenidas”, “indiferentes” y “temerarias”.

Los diez perfiles seleccionados para la realización de entrevistas en profundidad se muestran en la Ilustración 2.

Ilustración 2: Perfiles de empresas participantes en la fase de entrevistas en profundidad

SEGURIDAD DE LA INFORMACIÓN

Empresa 1

- Número de empleados: 65
- Actividad: Servicios de ingeniería y telecomunicaciones.
- Dispone de al menos cinco ordenadores, equipos portátiles y smartphones.
- No cuenta con personal dedicado en exclusiva a la seguridad de la información.
- Ha tenido algún incidente de seguridad y ha tomado medidas tras él.

Empresa 2

- Número de empleados: menos de 10
- Actividad: Servicios de publicidad y marketing.
- Dispone de al menos dos ordenadores
- Cuenta con personal dedicado exclusivamente a la seguridad de la información.
- Ha tenido algún incidente de seguridad y ha tomado medidas tras él.

Empresa 3

- Número de empleados: 92
- Actividad: Servicios empresariales
- Dispone de al menos dos ordenadores
- Dispone de empresa externa que gestiona los aspectos de seguridad de la información.
- Ha tenido algún incidente de seguridad y ha tomado medidas tras él.

Empresa 4

- Número de empleados: 3
- Actividad: Comercio
- Dispone de un ordenador.
- No dispone de personal dedicado a seguridad de la información.
- No ha tenido incidentes de seguridad.

Empresa 5

- Número de empleados: 25
- Actividad: Comercio y distribución.
- Dispone de más de 5 ordenadores, equipos portátiles y smartphones.
- Ha tenido algún incidente de seguridad y ha tomado medidas tras él.

CONTINUIDAD DE NEGOCIO

Empresa 6

- Número de empleados: 150
- Actividad: Distribución de software.
- Dispone de una estrategia de continuidad de negocio.

Empresa 7

- Número de empleados: 50.
- Actividad: Servicios a trabajadores.
- Las actividades críticas del negocio están identificadas.
- Ha sufrido en el último año un incidente de continuidad de negocio.
- No dispone de una estrategia de continuidad de negocio.

Empresa 8

- Número de empleados: 1.
- Actividad: Otros servicios.
- Las actividades críticas del negocio están identificadas.
- No dispone de una estrategia de continuidad de negocio.

Empresa 9

- Número de empleados: 5.
- Actividad: Servicios de informática.
- Las actividades críticas del negocio están identificadas.
- Dispone de una estrategia de continuidad de negocio.
- Con experiencias previas de incidentes con impacto en la continuidad de las operaciones de negocio.

Empresa 10

- Número de empleados: 100.
- Actividad: Transporte.
- Las actividades críticas del negocio están identificadas.
- Con experiencias previas de incidentes con impacto en la continuidad de las operaciones de negocio.
- Dispone de una estrategia de continuidad de negocio.

Fuente: INTECO

2.4 FASE 4: GRUPO DE TRABAJO FINAL CON EXPERTOS CUALIFICADOS

Por último, se han llevado a cabo la creación de un grupo de trabajo con expertos de diferentes ámbitos. Para la elección de la relación de expertos que formaron el grupo se ha tenido en cuenta principalmente su experiencia profesional, así como el cargo que ocupan dentro de la empresa (cargos con responsabilidad y conocimientos sobre la seguridad de la información).

Por otra parte también se consideró la diversidad de perfiles (distintos tipos de empresas y entidades, asociaciones empresariales) y su reputación dentro del sector. Así, estaban representadas la industria de la seguridad de la información, asociaciones de empresas del sector TIC, grandes empresas consumidoras y que imprimen un efecto tractor en la adopción de soluciones de seguridad, organismos de certificación, autoridades de control en el ámbito de la protección de datos personales, empresas proveedoras de servicios legales y servicios de consultoría y apoyo relacionados con la protección de datos personales en la empresa.

La relación de expertos participantes en el presente estudio es la siguiente:

- Emilio Aced (*Agencia de Protección de Datos de la Comunidad de Madrid*).
- Adrián Agudo (*Indra Sistemas*).
- César Alonso (*AUDISEC Seguridad de la Información*).
- Antonio Cimorra (*Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y Comunicación, de las telecomunicaciones y de los contenidos digitales - AMETIC*).
- Luis Fuertes (*Symantec Ibérica*).
- Ricard Martínez (*Asociación Profesional Española de Privacidad - APEP)*).
- Oscar Pastor (*Ingeniería de Sistemas para la Defensa de España - ISDEFE*).
- Pablo Pérez (*Observatorio de la Seguridad de la Información, del Instituto Nacional de Tecnologías de la Comunicación- INTECO*)
- José Ángel Valderrama (*Asociación Española de Normalización y Certificación - AENOR*).

Se llevó a cabo una sesión de debate, celebrada el día 28 de marzo de 2012 a las 16:30 horas, con una duración de 2,5 horas. El objetivo de este grupo final ha sido profundizar en los resultados obtenidos en el análisis anterior, así como recabar la opinión de estos expertos profesionales y expertos ligados al ámbito de la seguridad TIC y la continuidad de negocio en relación a las principales incidencias, tanto a nivel técnico como legal producidas en las empresas, así como la posible identificación de las principales recomendaciones para mitigar estas incidencias.

Para la consecución del objetivo, la metodología de trabajo durante la sesión ha consistido en la presentación de los resultados preliminares de la encuesta y la apertura de un turno de debate durante el que los expertos han aportado sus opiniones o consideraciones. Todo ello ha sido llevado a cabo con el control de un moderador.

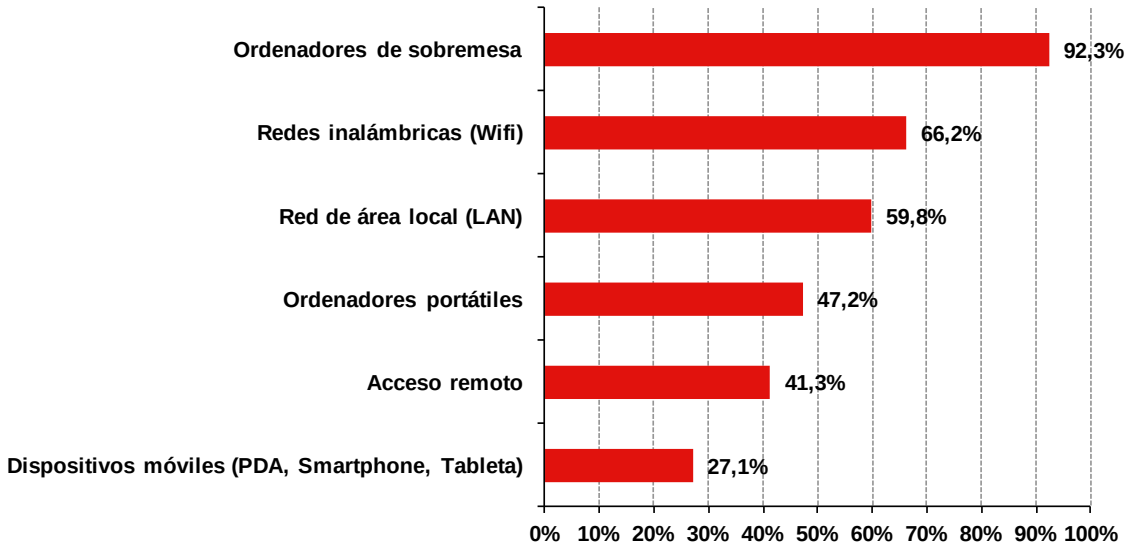
Con posterioridad a la celebración de la sesión, el análisis se ha basado en el estudio de la transcripción literal de las deliberaciones, que han sido examinadas, filtradas e integradas en el presente estudio.

3 HERRAMIENTAS TÉCNICAS Y PERSONAL DE SEGURIDAD

En el presente estudio, las empresas participantes muestran un notable uso de las TIC. El ordenador de sobremesa es una herramienta imprescindible en la actividad empresarial, con un 92,3% de penetración. El ordenador portátil está presente en un 47,2% de las empresas y dispositivos móviles como los smartphones, tabletas y PDAs, en un 27,1%. Las empresas señalan el recambio tecnológico (debido a la aparición de nuevos productos o también por incidentes de seguridad) como un factor que influye en sus negocios.

Otro indicador del nivel de la importancia de las TIC en la pequeña y mediana empresa española es la interconexión de sus equipos. Dos de cada tres organizaciones dicen tener interconectados sus equipos a través de una red wifi, mientras que la penetración de las redes de área local (LAN) se sitúa en el 59,8%. Finalmente, un 41,3% utiliza conexión a través de acceso remoto.

Gráfico 3: Distribución del uso de tecnologías TIC (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Dado el uso que realizan estas empresas de las nuevas tecnologías, en el presente apartado se estudia la percepción del colectivo participante en el estudio en cuanto a su grado de protección en materia de seguridad de la información.

Por ello, se estudian los recursos técnicos y humanos dedicados a la seguridad de la información, el grado de implantación de las herramientas en la empresa, la seguridad en los dispositivos móviles y en las redes inalámbricas, el personal dedicado a la seguridad, y la evolución de la inversión en seguridad.

En los capítulos posteriores, se complementa este diagnóstico con el análisis de las buenas prácticas para la protección y se examina la percepción sobre el conocimiento e implementación de planes y políticas de seguridad y continuidad de negocio.

El análisis parte de la opinión de los responsables de seguridad y continuidad de las empresas sobre los procedimientos y herramientas que permiten garantizar la integridad, disponibilidad y confidencialidad de la información. Los resultados se complementan con un análisis segmentado por tamaño o sector económico con el objeto de aportar mayor riqueza al estudio.

La información obtenida en el trabajo de campo cuantitativo se explica, en los casos en que es posible, con las aportaciones de los expertos y responsables de seguridad que han participado en el estudio.

Por último, señalar que en los casos en que la información recabada lo permite, se realiza un análisis longitudinal, utilizando para ello los resultados obtenidos en estudios previos de INTECO, así como de otras fuentes documentales[13].

3.1 HERRAMIENTAS DE SEGURIDAD EN LA EMPRESA ESPAÑOLA: IMPLANTACIÓN Y MOTIVACIÓN

Como se desprende del análisis, las empresas afirman disponer de diversas herramientas de seguridad para proteger sus equipos, con un notable nivel de adopción en líneas generales.

Este es el caso de las soluciones asociadas a la seguridad en la navegación, encabezadas por los antivirus y/o antiespías (96,1%), seguidos de los cortafuegos (75,4%), los programas antispam (75,3%) y las herramientas de bloqueo de ventanas emergentes (71,5%).

Por detrás de estas se sitúan herramientas o medidas que implican la participación del usuario, como la eliminación de archivos temporales y cookies (67,4%) y aquellas que aportan funcionalidades adicionales a las tradicionales que ofrece una solución antimalware, como los sistemas de control de intrusión (52,9%), los plugins o complementos de seguridad para el navegador (51,4%) y el cifrado de datos (34,1%). Tan solo el 2,4% de las organizaciones consultadas señaló no contar con ninguna de las indicadas.

La percepción de las empresas encuestadas sobre la incorporación de soluciones de seguridad se ajusta en líneas generales a la realidad, según los expertos consultados en el marco del estudio. En este sentido, las organizaciones suelen adquirir soluciones paquetizadas, que cuentan con una serie de funcionalidades. Algunas son percibidas porque son conocidas ampliamente (antivirus / antiespías, cortafuegos[14]), otras son declaradas en menor medida aunque están en esos paquetes (antispam, eliminación de archivos temporales y cookies). Únicamente en el caso del cifrado de datos se presume una menor penetración de la obtenida en la encuesta.

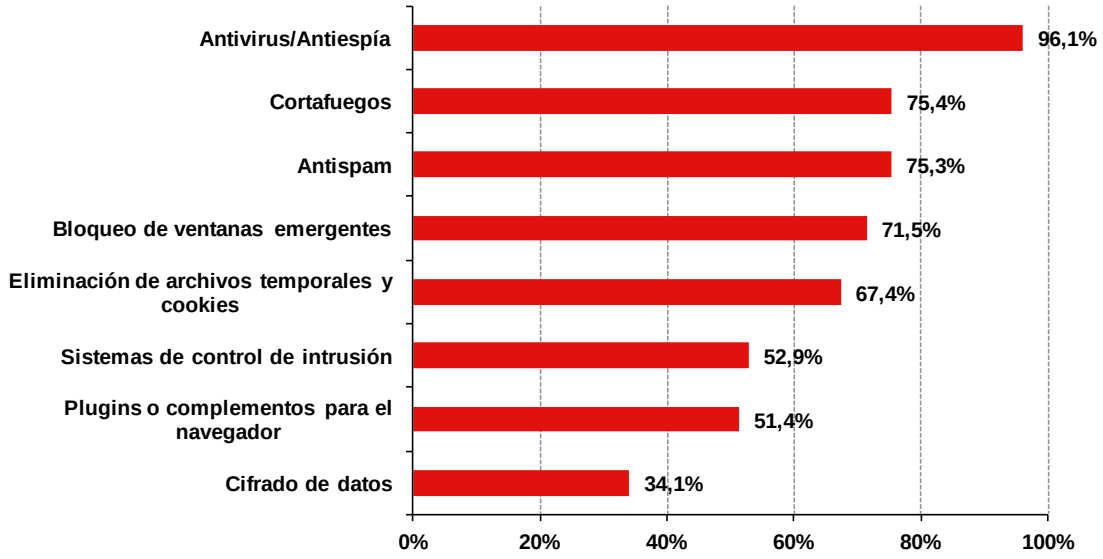
[13] Ver apartado ANEXO I.

[14] Según el estudio *Las Tecnologías de la Información y las Comunicaciones en la empresa española*, de AETIC-Everis (2011), el 96,3% de las empresas españolas dispone de un programa antivirus y el 81,2% de sistemas de cortafuegos. Disponible en: http://www.everis.com/spain/WCRepositoryFiles/Estudio_everis_AMETIC.pdf

En este sentido, las empresas participantes en la entrevista en profundidad señalan que el cifrado de datos es inherente a la utilización de servicios TIC como la banca electrónica, lo que puede influir en la elevada proporción de empresas que considera que utiliza esta herramienta.

Este colectivo percibe la existencia de riesgos que no solucionan las herramientas actuales, como por ejemplo el hacking o el spam. Además, demandan la integración de la solución y configuración de seguridad en la subcontratación de soluciones tecnológicas, por ejemplo, al hablar de servicios de *cloud computing*.

Gráfico 4: Nivel de implantación declarado de soluciones de seguridad en la empresa (%)



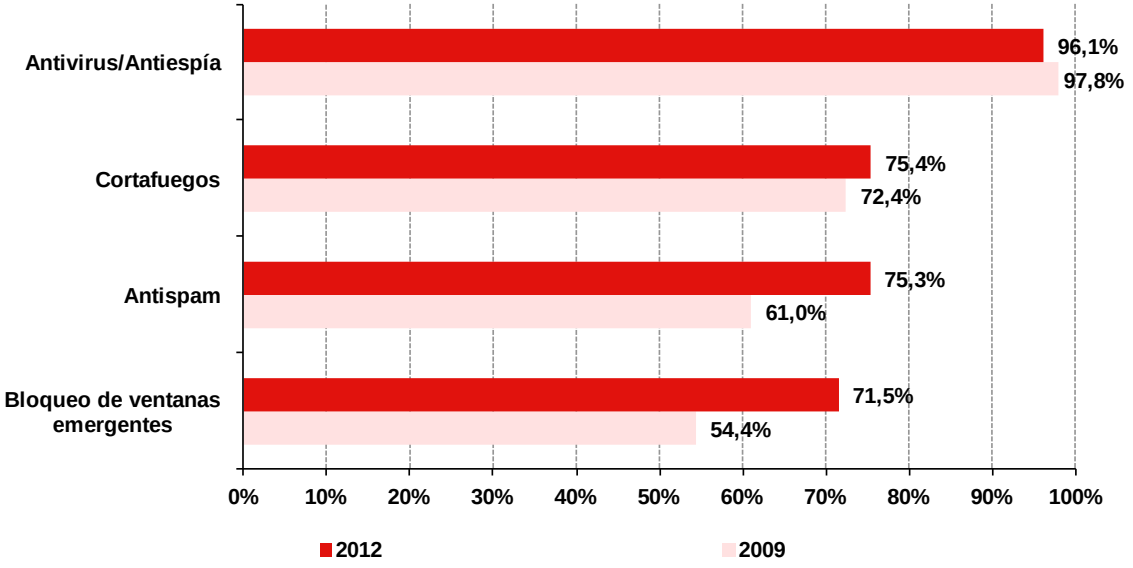
Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

La evolución en el nivel de penetración de las principales soluciones desde 2009[15] a la actualidad es positiva. Las soluciones más comunes, como los cortafuegos o los antivirus/antiespía muestran valores similares en ambos periodos. Sin embargo, algunas herramientas declaradas en menor medida en 2009 experimentan un ascenso en su implantación, como el antispam (que pasa de un 61% en 2009 a un 75,3% en 2012) o el bloqueo de ventanas emergentes (de un 54,4% a un 71,5%).

Es importante tener en cuenta la incorporación de empresas de mayor dimensión en presente estudio, ya que el universo considerado varía respecto al del anterior. En el año 2009 estaba constituido por empresas de hasta 50 empleados, mientras que en la edición actual está conformado por empresas de hasta 250 empleados.

[15] Fuente: Ver nota al pie 3.

Gráfico 5: Nivel de implantación declarado de las principales soluciones de seguridad Evolución 2009-2012 (%)



Base 2012: total empresas (n=1.144) *Fuente: INTECO*
Base 2009: total empresas (n=2.206)

La preferencia por las distintas herramientas no varía en función del tamaño (las herramientas más declaradas son antivirus/antiespía, cortafuegos y antispam), aunque sí el grado de utilización, mayor en las medianas empresas.

Tabla 3: Disponibilidad de herramientas para proteger equipos y sistemas según tamaño de las empresas (%)

Soluciones	Microempresa	Pequeña empresa	Mediana empresa
Antivirus/Antiespía	96,1	97,6	98,2
Cortafuegos	74,9	82,6	90,4
Antispam	74,9	80,6	93,6
Bloqueo de ventanas emergentes, banners publicitarios	71,4	72,7	80,2
Eliminación de archivos temporales y cookies	67,2	69,3	73,9
Sistemas de control de intrusión	52,5	56,8	66,7
Plugins o complementos de seguridad para el navegador	51,0	57,1	65,3
Cifrado de datos	33,4	45,7	54,5

Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

La tabla siguiente muestra cuáles son las razones aportadas por las empresas para justificar la no disponibilidad de las distintas herramientas de seguridad. Una particularidad a tener en cuenta, es que la base de cálculo se constituye en cada caso por las empresas que dicen no utilizar cada solución, por lo que los datos deben tomarse meramente como orientativos.

Las empresas que han indicado no disponer de las distintas herramientas de seguridad alegan diferentes motivos para no implantarlas, principalmente el desconocimiento y la falta de necesidad[16]. Otras consideraciones, como el coste, la sensación de ineficacia o de entorpecimiento en el funcionamiento del equipo, aparecen en menor medida y de forma desigual en función de la herramienta de que se trate en cada momento. Asimismo, sorprende el elevado porcentaje de empresas que no dan una respuesta.

En función de cada herramienta se encuentran diferencias que se exponen a continuación. El desconocimiento es mayor en las empresas que no utilizan sistemas de control de intrusión, plugins o cortafuegos, mientras que las que no disponen de antivirus/antiespía y antispam son las que alegan no necesitar las herramientas y soluciones de seguridad. Por último destaca que el entorpecimiento que provocan las herramientas es un motivo destacado entre las organizaciones que no tienen antivirus/antiespía.

Tabla 4: Motivos señalados por las empresas para no utilizar las herramientas y soluciones de seguridad (%)

Soluciones	% empresas que no utilizan en la actualidad	Motivos						
		No conoce	No necesita	Precio	Ineficaces	Entorpecen	Otros	No contesta
Antivirus / Antiespía	3,9	2,3	**39,6**	0,4	5,1	17,4	14,9	20,3
Cortafuegos	24,6	**35,6**	27,2	3,2	0,8	2,8	0,2	30,2
Antispam	24,7	28,0	**38,8**	0,1	0,8	3,8	0,2	28,3
Plugins	48,6	**37,0**	28,4	0,5	0,5	2,0	0,4	31,2
Bloqueo de ventanas emergentes	28,5	**33,3**	29,7	0,0	0,9	2,9	0,2	33,0
Sistemas de control de intrusión	47,1	**38,0**	26,0	1,4	0,4	2,1	0,2	31,9
Cifrado de datos	65,9	35,1	**35,2**	0,4	0,5	1,6	0,8	26,4
Eliminación de archivos temporales y cookies	32,6	29,1	**32,5**	0,7	1,1	3,1	1,5	32,0

Base: empresas que no utilizan las herramientas y soluciones de seguridad *Fuente: INTECO*

[16] Según el Estudio *II Barómetro Internacional de Seguridad en las Pymes* Panda Security (2010) el principal problema para no introducir un sistema de seguridad en las empresas españolas es la falta de necesidad. Disponible en: http://www.inteco.es/studyCategory/Seguridad/Observatorio/Biblioteca/barometro_internacional_PYMES_panda

En términos generales, la percepción del grado de implantación de las herramientas de seguridad es notable, puesto que todas las medidas, a excepción del cifrado de datos, son declaradas por más de la mitad de las empresas. Es especialmente destacado el uso de herramientas disponibles en soluciones en paquete, como antivirus y cortafuegos, que están más extendidas que el resto.

No obstante, las empresas muestran desconocimiento, desinterés y falta de recursos a la hora de aplicar herramientas más allá de las tradicionales. Los expertos y los responsables de seguridad de las empresas que han colaborado en el estudio consideran que se debe trabajar para ampliar el grado de integración de las herramientas, con medidas como la sensibilización por parte de los organismos que trabajan directamente con este colectivo.

3.2 SEGURIDAD EN DISPOSITIVOS MÓVILES Y COMUNICACIONES INALÁMBRICAS

Los dispositivos móviles cada vez tienen más presencia en las empresas. Según McAfee[17], en 2010 siete de cada diez organizaciones dependían en mayor medida de los móviles que 12 meses antes. La extensión del uso y la creciente complejidad de este tipo de dispositivos (con funcionalidades como la transmisión de datos, el almacenamiento de información o la conexión a Internet) implican la necesidad de garantizar su protección.

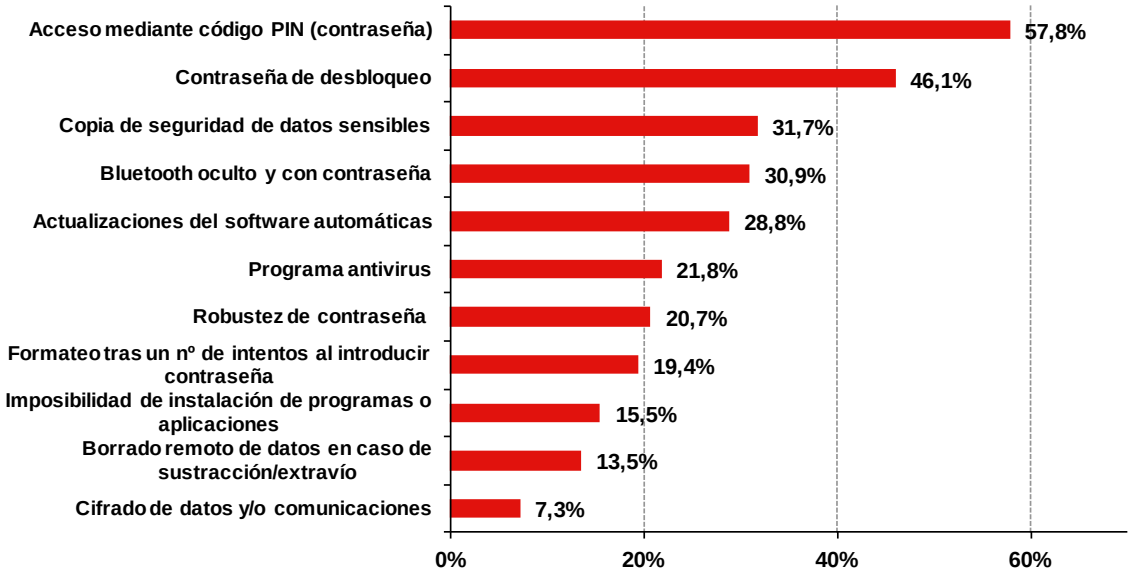
Así, como muestra el siguiente gráfico, las empresas disponen de diversas medidas de seguridad para sus dispositivos móviles. Entre las más mencionadas, destaca el acceso mediante código PIN (un 57,8%), y las contraseñas de desbloqueo (un 46,1%).

Menos de un tercio de las empresas con estos dispositivos móviles señalan otras medidas como la realización de las copias de seguridad de datos sensibles (31,7%), Bluetooth oculto y con contraseña (30,9%), actualizaciones del software automáticas (28,8%), y los programas antivirus (21,8%). Entre las menos utilizadas se sitúan el cifrado de datos (sólo el 7,3% de las empresas afirman disponer de este sistema), el borrado de datos en remoto (13,5%) o la imposibilidad de la instalación de programas o aplicaciones (15,5%).

Por último, se observa que las empresas de menor tamaño declaran utilizar principalmente medidas más difundidas, y que habitualmente están preinstaladas en los propios dispositivos y automatizadas. En cambio, las medianas recurren a otras más complejas y muestran un mayor grado de preocupación por el acceso a los dispositivos y a los datos.

[17] Fuente: MCAFEE (2010) *"Movilidad y seguridad: impresionantes oportunidades desafíos profundos"*, En el estudio se realizaron 1.500 encuestas a organizaciones de 14 países entre los que se incluía a España. Las encuestas se realizaron a responsables de las tecnologías de la información de empresas de más de 100 trabajadores.

Gráfico 6 : Medidas de seguridad utilizadas/instaladas en los dispositivos móviles (%)



Base: Empresas que disponen de dispositivos móviles (n=459) *Fuente: INTECO*

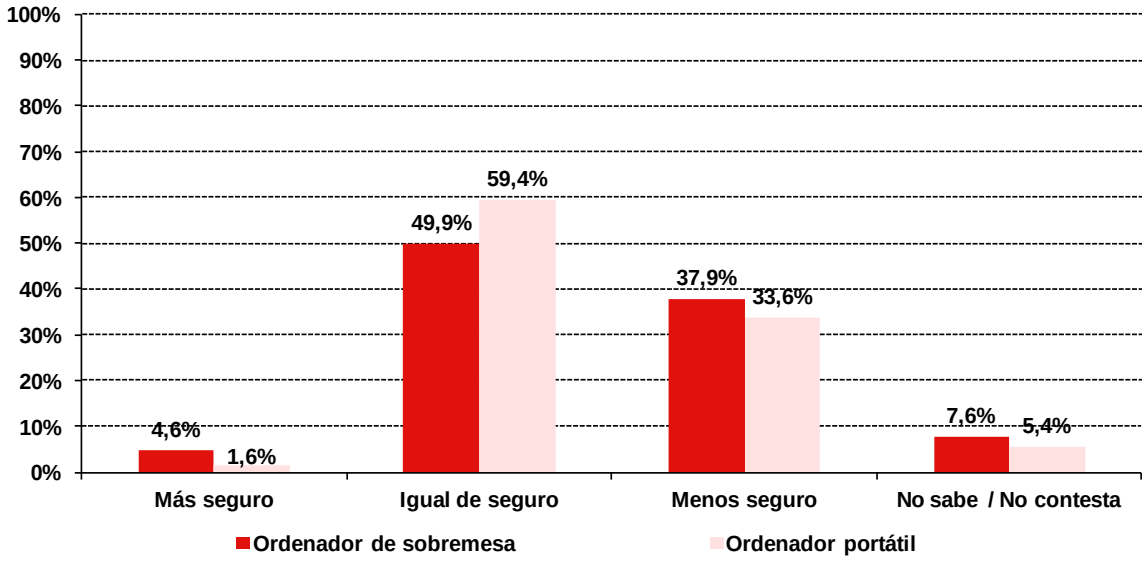
En términos generales las empresas integran en mayor medida elementos de seguridad en los equipos informáticos que en los dispositivos móviles.

Este es el caso de los programas antivirus/antiespía, con una penetración casi total en ordenadores (un 96,1%) y menor en dispositivos móviles un (un 21,8%). La diferencia también es acusada en el caso de las copias de seguridad (un 88,2% declara realizarlas en los ordenadores, frente a un 31,7% en los móviles).

El Gráfico 7 muestra la percepción de las empresas al comparar el nivel de seguridad de los dispositivos móviles frente a equipos fijos y portátiles. A este respecto hay que señalar que el porcentaje de empresas que han sufrido un incidente de seguridad es muy similar tanto en el caso de los dispositivos móviles como en el de los ordenadores.

Para más de la mitad de las empresas, los dispositivos móviles no implican menor seguridad con respecto al resto de equipos: para un 49,9% son igual de seguros que un ordenador fijo, encontrando mayor similitud con los ordenadores portátiles (59,4%). No obstante, algo más de un tercio considera que son menos seguros, especialmente frente al ordenador de sobremesa.

Gráfico 7: Percepción del nivel de seguridad de los dispositivos móviles frente equipos fijos y portátiles (%)



Base: Empresas que disponen de ordenadores de sobremesa o portátiles (n=378) *Fuente: INTECO*

La incorporación de los dispositivos móviles en las empresas es relativamente reciente, lo que puede explicar que el nivel de concienciación sobre la necesidad de disponer de herramientas de protección sea menor.

Sin embargo, las funcionalidades que aportan son cada vez más indispensables y los atacantes, conscientes de esa necesidad, perfeccionan constantemente sus ataques dirigidos a los dispositivos móviles. El impacto que para la empresa puede ocasionar la pérdida o deterioro de la información almacenada en los terminales genera la necesidad de implementar y mantener actualizados las herramientas de seguridad en estos dispositivos. Junto con esta incorporación, deben llevarse a cabo medidas de sensibilización y concienciación que acompañen a las anteriores.

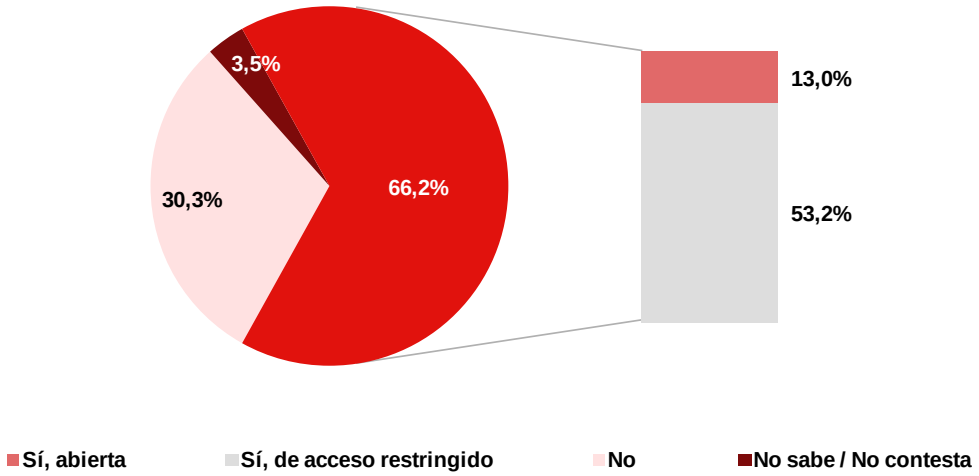
Como hemos visto, las empresas cada vez más requieren de tecnologías y equipos que aporten un componente de movilidad y accesibilidad a su actividad de negocio. Además de los dispositivos móviles, las comunicaciones a través de redes inalámbricas[18] contribuyen a este propósito, por lo que cada vez están más extendidas entre las pequeñas y medianas empresas.

Así, dos de cada tres negocios manifiestan disponer de una conexión wifi (un 13% abierta y un 53,2% de acceso restringido), como se aprecia en el Gráfico 8. La penetración es superior en las

[18] Las conexiones inalámbricas) proporcionan el acceso a Internet sin necesidad de cables o puntos de acceso cercanos. La nomenclatura IEEE 802.11, conocida popularmente como wifi, es un conjunto de estándares de protocolos para comunicaciones inalámbricas. Dado que dispositivos como ordenadores portátiles, tabletas o móviles disponen de capacidad para conectarse a Internet a través de wifi, la conexión puede ser ubicua e instantánea en cualquier lugar.

empresas de mayor tamaño, lo que puede ser debido a la percepción de que las comunicaciones inalámbricas son "más difíciles de gestionar y proteger", opinión recogida en las entrevistas en profundidad a los responsables de seguridad de las compañías participantes.

Gráfico 8: Servicios de red inalámbrica o wifi declarados por las empresas (%)



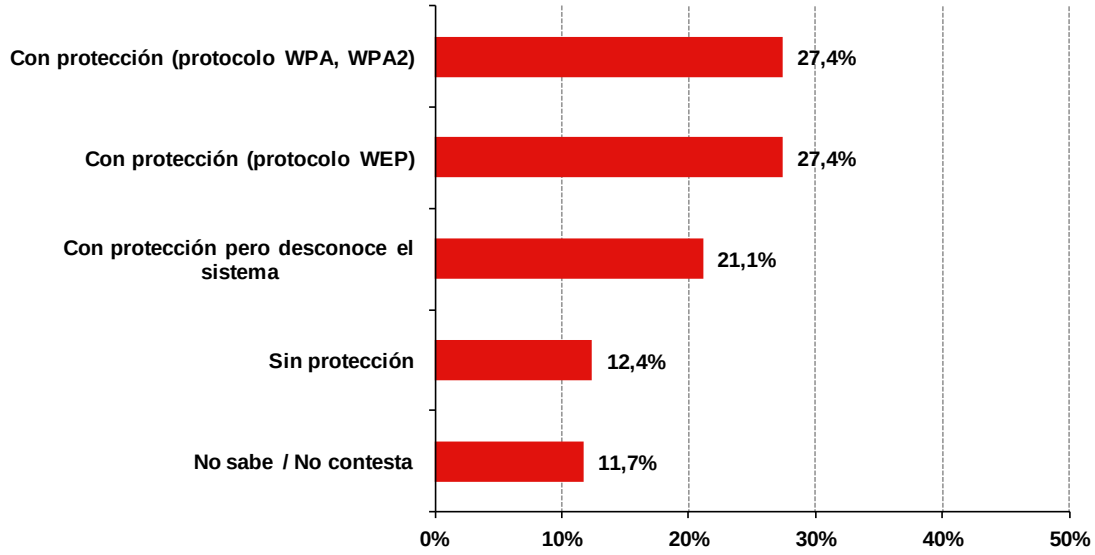
Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Las funcionalidades que aportan las redes wifi posibilitan también que surjan ataques e incidentes de seguridad. De cara a determinar la protección que las empresas aplican a sus redes inalámbricas, se analiza el grado de penetración de sistemas de cifrado para wifi: WEP, WPA y WPA2. Este cifrado debe ser robusto y estar avalado por una contraseña fuerte.

El estándar WPA es sólido y los proveedores lo incluyen cada vez más como método de cifrado por defecto en los *routers*. La segunda versión de este estándar, WPA2, aporta mayor robustez, por lo que es más recomendable. El estándar WEP (estático) es un método de cifrado anterior al WPA (dinámico) y se considera obsoleto.

De las empresas que disponen de redes wifi abiertas, los protocolos WPA/WPA2 y WEP tienen la misma penetración (un 27,4%) y un 21,1% desconocen cuál es el sistema utilizado, pero afirman que su red está protegida. Por último, un 11,7% desconocen si existe alguna medida de seguridad en su red y el 12,4% afirma que no existe esta garantía.

Gráfico 9 : Medidas de seguridad en redes wifi de la empresa (%)



Base: Empresas que disponen de red Wifi (n=129) *Fuente: INTECO*

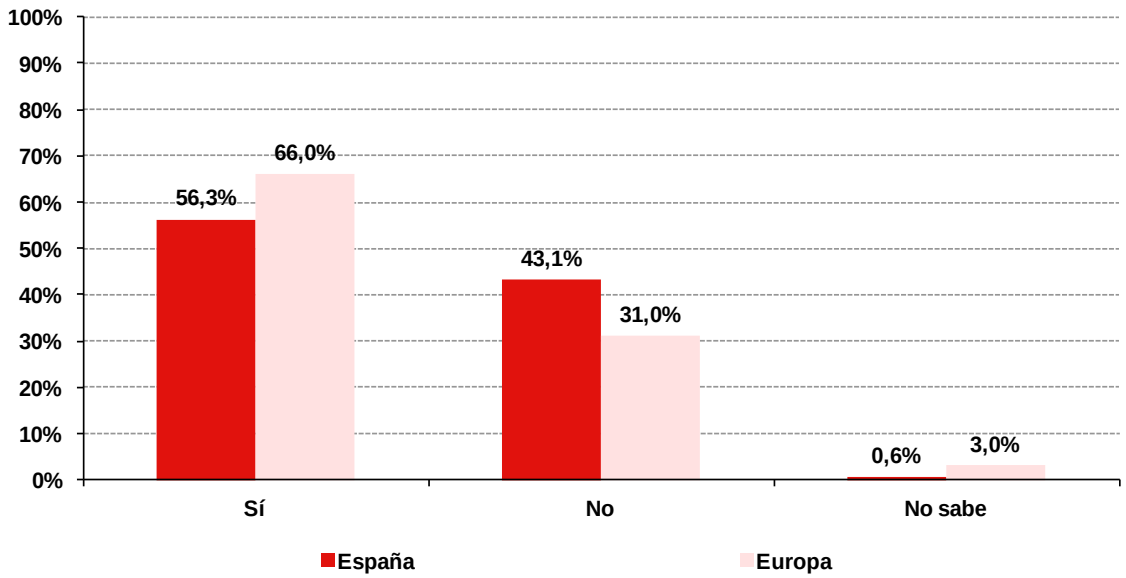
La elección de la protección de la red wifi en igual proporción en ambos sistemas (WPA y WEP) revela que las empresas no conocen suficientemente los estándares de cifrado y la protección que ofrece cada uno. Parte del desconocimiento de las empresas tanto de la protección de la red wifi, como de los protocolos existentes puede deberse, en opinión de los expertos, a que la seguridad se encomienda al proveedor de los servicios de Internet.

3.3 PERSONAL DEDICADO A LA SEGURIDAD DE LA INFORMACIÓN

La adecuada gestión de la información en la organización depende en mayor o en menor medida de todos sus miembros y del uso de los recursos disponibles. Por ello, además de analizar las herramientas de seguridad que utilizan las empresas, otro de los ejes principales sobre los que se centra el presente apartado es el personal dedicado a la seguridad de la información.

Como indica el siguiente gráfico, el grado de disponibilidad de profesionales encargados de la seguridad de la información en las empresas españolas se acerca a los niveles europeos (un 56,3% de organizaciones españolas disponen de estos perfiles, frente a un 66% de empresas europeas), aunque es necesario continuar avanzando para salvar esta diferencia.

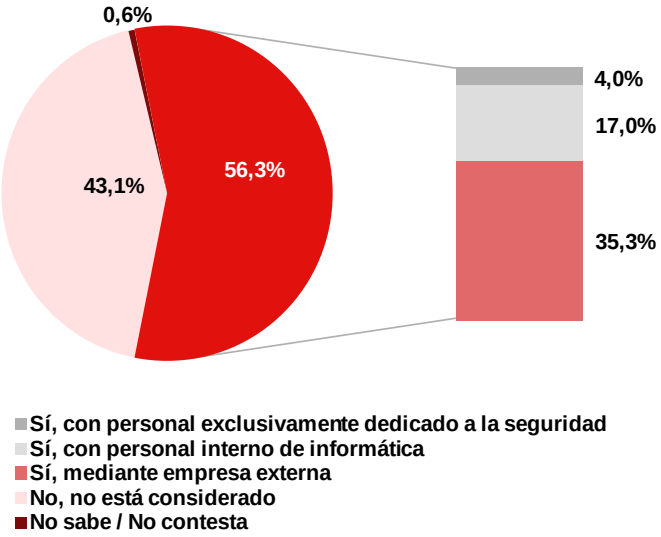
Gráfico 10: Empresas que afirman contar con personas dedicadas a la seguridad de la información. Comparativa europea (%)



Base: España 2012 total empresas (n=1.144) *Fuente: INTECO (España)*
Base: Europa 2010 (n= 6.413) *Fuente: Panda Security (Europa)*

Un análisis más exhaustivo muestra que en un 4,0% de las organizaciones estos profesionales internos se dedican exclusivamente a la seguridad, mientras que en un 17,0% compaginan esta actividad con funciones relacionadas con la informática. Asimismo, es reseñable el porcentaje de empresas que externaliza esta función (35,3%). Por el contrario, un 43,1% afirma no incluir un profesional de seguridad en su equipo humano.

Gráfico 11: Disponibilidad de personal dedicado a la seguridad de la información (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

El análisis realizado en función del tamaño indica que existe una mayor probabilidad de encontrar profesionales de seguridad en las empresas de mayor dimensión (un 62,8% en las medianas empresas), ya sea en exclusiva (12,4%) o compaginando otras funciones de informática (50,4%). Por su parte, las pequeñas empresas recurren, principalmente, a la gestión externa de la seguridad. Es especialmente significativo que un 44,8% de las microempresas no consideran en su plantilla a personas dedicadas a la seguridad de la información.

Tabla 5: Disponibilidad de personal dedicado a la seguridad según tamaño de empresa (%)

Personal de seguridad	Microempresa	Pequeña empresa	Mediana empresa
Sí, con personal exclusivamente dedicado a la seguridad	3,9	5,5	12,4
Sí, con personal interno de informática	15,9	32,7	50,4
Sí, mediante empresa externa	34,9	44,3	29,5
No, no está considerado	44,8	15,8	7,2
No sabe/ No contesta	0,5	1,7	0,5

Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Estos resultados se explican tanto por los recursos disponibles, estrechamente relacionados con el tamaño de la empresa, como por prioridad otorgada a la seguridad de la información.

Según señalan los expertos, los proveedores de servicios para este colectivo de empresas son los encargados en muchos casos de incorporar la seguridad en sus servicios, como fórmula de

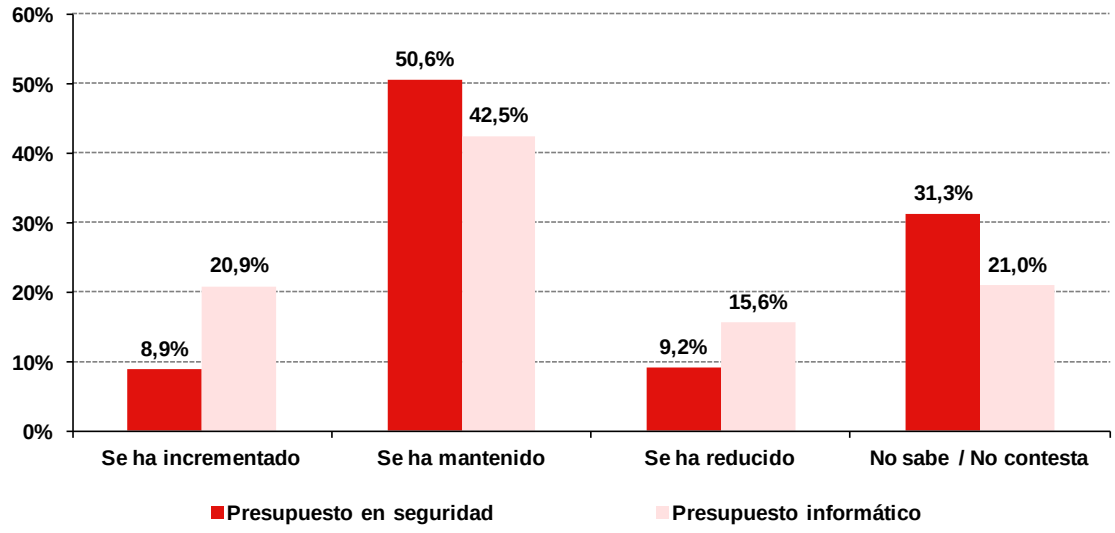
diferenciación y excelencia, por lo que la empresa no percibe que su implicación sea mayor. Por su parte, como indican los responsables de seguridad entrevistados, en las empresas de menor tamaño la prioridad del administrador de los sistemas informáticos es dar servicio y, de forma secundaria, organizar la seguridad de la información. También señalan que, al confiar en recursos externos, "garantizan que el profesional tenga un conocimiento más profundo y actualizado".

3.4 ESTRATEGIA CORPORATIVA EN SEGURIDAD E IMPLICACIÓN DE LA DIRECCIÓN

El factor económico es clave a la hora de establecer una estrategia de seguridad en la empresa. La evolución de la inversión en el último año, tanto en informática como en seguridad de la información, se muestra en general bastante estable. Así, un porcentaje importante de negocios mantienen el presupuesto un año más (un 42,5% en informática en general y un 50,6% en seguridad de la información[19]), mientras que un 20,9% considera que ha incrementado la partida destinada a informática y un 8,9% la relativa a seguridad.

Esta evolución denota que las empresas consideran en cierta medida que la inversión en seguridad e informática es necesaria, aunque no existe una apuesta clara o incrementos más acusados.

Gráfico 12: Valoración del presupuesto en seguridad e informática en comparación con el año anterior (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

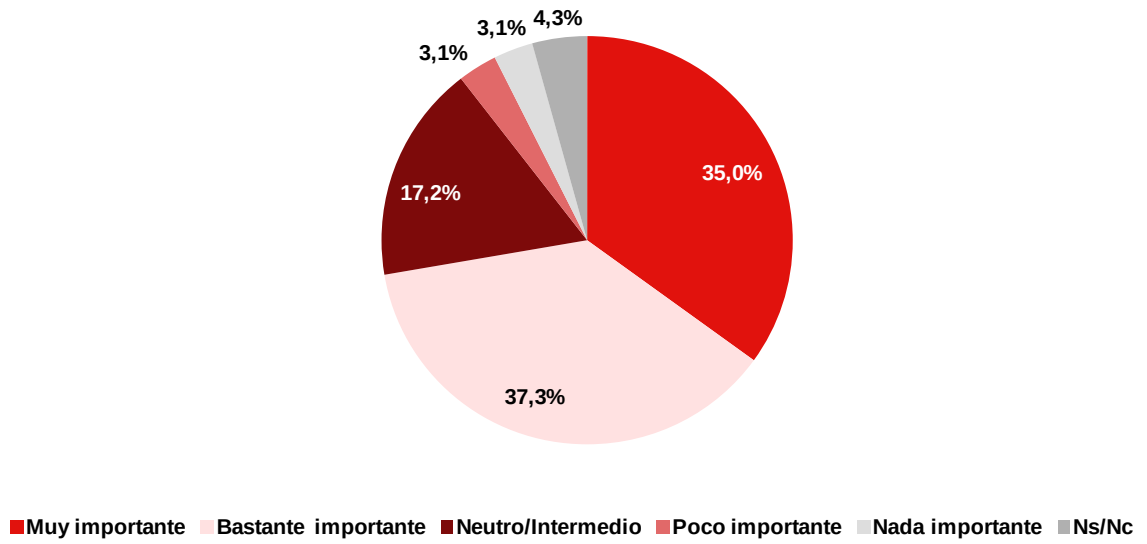
[19] Según el II Barómetro Internacional de Seguridad en PYMES, Panda (2010), el 52% de las empresas españolas declaran que su presupuesto de seguridad se ha mantenido con respecto al año anterior, dato que es el 45% en el conjunto de Europa.

Relacionado con lo anterior, la importancia que concede la Dirección de las empresas a la seguridad de la información propicia el impulso de estas actividades dentro de la organización y, consecuentemente, en el conjunto del tejido empresarial español.

Con relación a este aspecto, parece confirmarse que los órganos directivos de las empresas valoran positivamente la protección de las TIC como parte de la actividad. Así, un porcentaje destacado (un 72,3%) considera que es muy o bastante importante y un 17,2% se muestra indiferente. Por el contrario, un 6,2% dan una valoración negativa.

Al comparar estos datos con los del análisis anterior, se observa que esta valoración positiva de la seguridad no se traduce necesariamente en una mayor dotación presupuestaria.

Gráfico 13: Nivel de importancia que la dirección de la empresa otorga a la seguridad de la información (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

4 BUENAS PRÁCTICAS DE SEGURIDAD

La seguridad de la información en las empresas debe incluir, además de los recursos necesarios, la realización de buenas prácticas. La importancia de estos hábitos radica en su capacidad para hacer frente a una incidencia de seguridad, aliviando las posibles consecuencias.

De forma no exhaustiva, en el presente apartado se estudian algunas de las prácticas que están a disposición de las entidades: realización de copias de respaldo de los datos, la actualización de programas y sistemas, el establecimiento de medidas de control de acceso o el fomento de hábitos prudentes entre el personal de la organización.

4.1 COPIAS DE SEGURIDAD

La información almacenada en los equipos y sistemas es un activo de gran valor para las organizaciones, por lo que una adecuada gestión de la información es cada vez más importante, sobre todo en relación a los datos más sensibles (información estratégica, datos personales, referencias de propiedad intelectual, etc.).

Dentro de las actuaciones contempladas en una adecuada gestión de la información, se encuentra la realización de copias de respaldo de la información o *backups*. En este sentido, la normativa sobre protección de datos de carácter personal[20] establece, para aquellas empresas que dispongan de ficheros automatizados con datos de esta naturaleza, la obligatoriedad de realizar copias de respaldo al menos, semanalmente, así como de establecer procedimientos que oriente a la recuperación efectiva de la información.

Las medidas de seguridad sobre copias de respaldo afectan exclusivamente a ficheros automatizados, independientemente de su nivel, si bien el art. 102 establece obligaciones adicionales para realizar copias de respaldo de ficheros de nivel alto.

Esta práctica debe acompañarse de las medidas necesarias que aseguren la disponibilidad, integridad y confidencialidad de la información en cualquier momento, como por ejemplo, la disposición de estas copias de seguridad en un lugar distinto al de trabajo, con el fin de evitar una pérdida irreversible en caso de producirse un incidente grave.

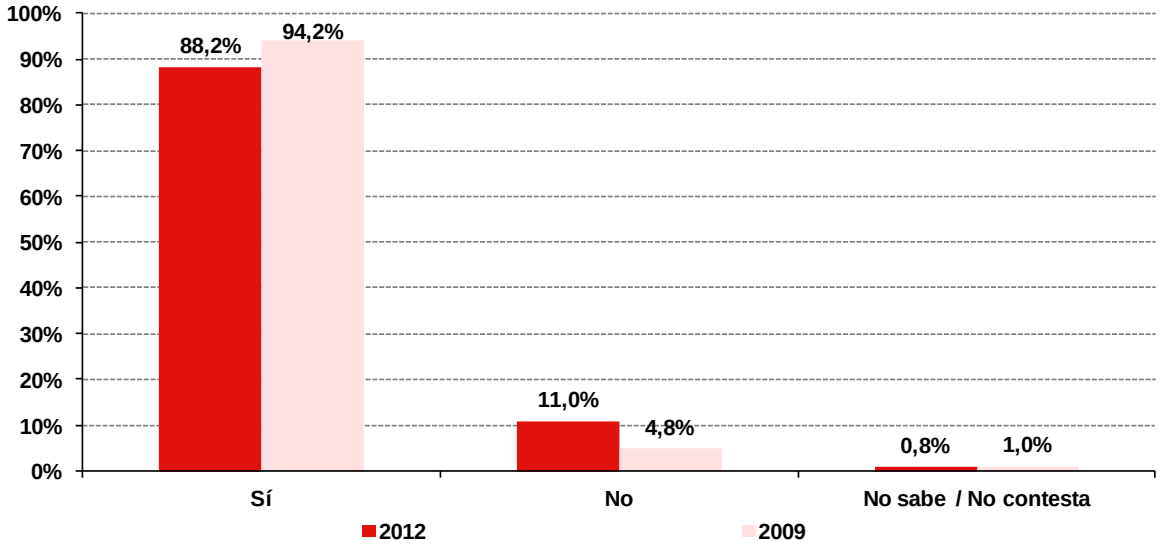
Como muestra el Gráfico 14, la importancia de la medida se refleja en la adopción mayoritaria por las empresas, tendencia que se mantiene con respecto a datos anteriores (un 88,2% en 2012 y un 94,2% en 2009 declaran realizar *backup* de la información). Los datos de 2009 están realizados en base a empresas hasta 50 trabajadores, mientras los datos de 2012 se refieren a organizaciones de hasta 250 trabajadores.

En función del tamaño, es significativo que las pequeñas y medianas empresas realizan copias de seguridad en similar proporción (un 97,5% y un 97,2%, respectivamente). Las microempresas realizan backups en menor medida (87,6%), debido probablemente, tanto a una menor

[20] Artículo 94 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, Ley 15/1999, de 13 de diciembre.

sensibilización, como a la menor percepción de los riesgos derivada del menor volumen de datos manejado. En todo caso, las empresas que han participado en las entrevistas de seguridad consideran esta medida como "imprescindible".

Gráfico 14: Evolución percibida de la realización de copias de seguridad (%)



Base 2012: Total empresas (n=1.144) *Fuente: INTECO*
Base 2009: Total empresas (n=2.206)

La puesta en práctica de esta medida debe responder a una planificación ajustada a las necesidades de la empresa. Por ello, es interesante observar entre las empresas que realizan copias de respaldo (n=1.081) la frecuencia, la tipología, el lugar de almacenamiento así como el control del acceso a estas copias.

El Gráfico 15 muestra que en el 31,1% de las empresas se realizan *backups* con una frecuencia semanal y en el 32,4% realizan este gesto todos los días. Sin embargo, es destacable que el 20,7% declara ampliar este periodo a una vez al mes, lo cual dificulta la recuperación de la información más reciente en caso de que se produzca un incidente de seguridad.

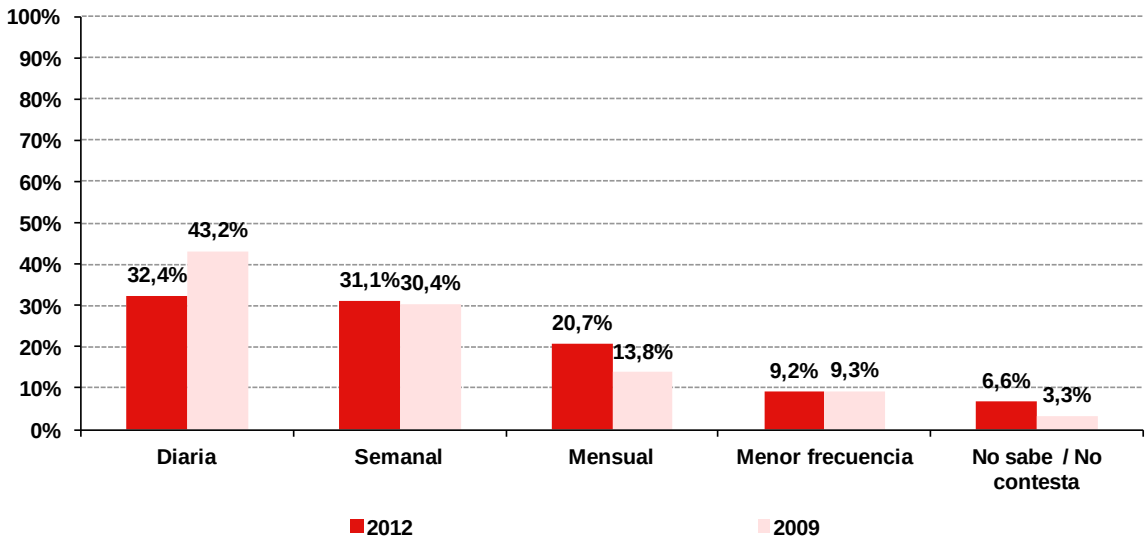
El análisis longitudinal de los datos con respecto a 2009 indica una cierta relajación en la frecuencia con la que se realizan las copias.

Se aprecia una relación directa entre el tamaño de la empresa y la frecuencia de duplicación de la información en *backups*. En tres cuartas partes de las medianas empresas el intervalo es diario, mientras que en las más pequeñas (de uno a diez trabajadores), la proporción se reduce al 30,3%.

En cuanto a los posibles motivos que expliquen esta relajación, algunas empresas alegan que "no utilizan los equipos informáticos de forma continua, por lo que no requieren aumentar la frecuencia con la que hacen copias de seguridad". Por su parte, las empresas medianas suelen disponer de

políticas específicas destinadas a la recuperación de la información, debido a la mayor cantidad de datos que manejan.

Gráfico 15: Evolución de la frecuencia declarada en la realización de copias de seguridad 2009-2012 (%)

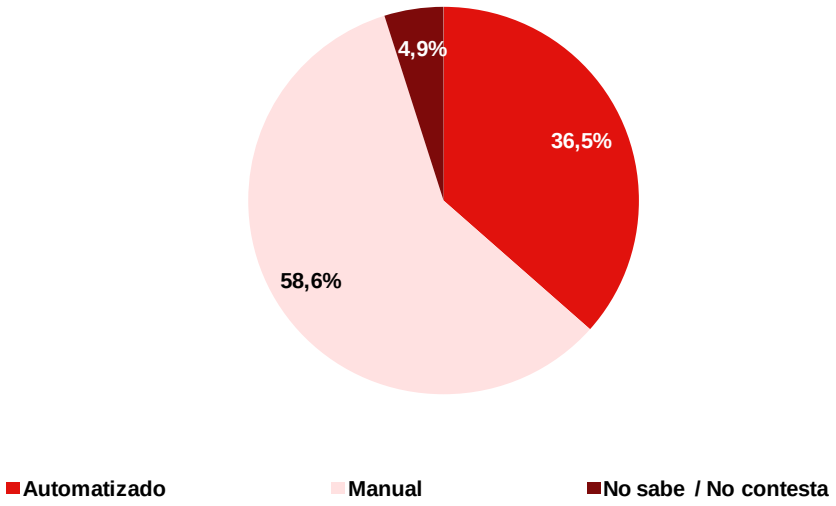


Base: Empresas que realizan copias de seguridad (n=1.081) *Fuente: INTECO*

Las empresas se muestran divididas a la hora de decantarse por el sistema utilizado para la realización de copias de seguridad. Un 58,6% opta por hacerlas manualmente, mientras un 36,5% prefiere sistemas automatizados.

Por tamaño, del análisis se desprende que los métodos manuales son más frecuentes entre las empresas más pequeñas, mientras que las empresas de mayor tamaño prefieren ampliamente la realización automática.

Gráfico 16: Tipo de configuración declarada a la hora de realizar copias de seguridad (%)



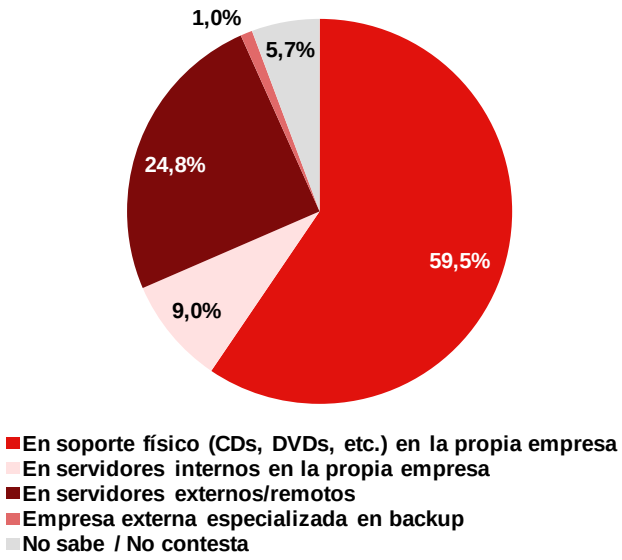
Base: Empresas que realizan copias de seguridad (n=1.081) *Fuente: INTECO*

La ubicación final de las copias es también un aspecto importante. No habrá posibilidad de recuperar la información almacenada si ocurre un incidente que afecta a la fuente original y a la copia, por lo que los expertos en seguridad aconsejan que las copias de seguridad se coloquen en una ubicación distinta, a poder ser en un lugar distinto al de la propia empresa.

Sin embargo, solo 1 de cada 4 empresas que realiza copias de seguridad utiliza una ubicación externa, frente a un 68,5% que almacenan las copias de seguridad en la propia empresa, ya sea en soportes físicos como CDs, DVDs, etc. (un 59,5% así lo afirma), o en servidores internos (un 9,0%). Únicamente un 1% recurre a empresas externas especializadas para esta conservación.

Por último, las empresas de mayor tamaño muestran una confianza superior en la utilización de servidores remotos y en la externalización de la gestión de las copias de respaldo.

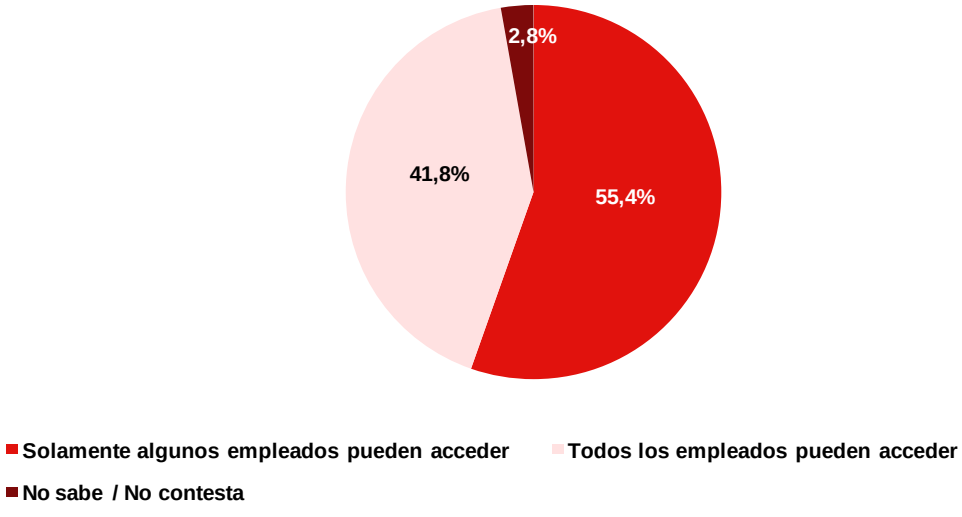
Gráfico 17: Lugar donde las empresas almacenan las copias de seguridad (%)



Base: Empresas que realizan copias de seguridad (n=1.081) *Fuente: INTECO*

Por último, las organizaciones no siempre establecen permisos para el acceso de determinados empleados a las copias de seguridad. Así, un 55,4% de las empresas consultadas señalan que sí aplican esta medida, mientras que un 41,8% no establece restricciones de acceso. Existe una relación directa entre el tamaño de la empresa y la existencia de controles de acceso a los *backups*.

Gráfico 18: Empresas que afirman aplicar restricciones en el acceso a *backups* (%)



Base: Empresas que realizan copias de seguridad (n=1.081) *Fuente: INTECO*

En términos generales, la realización de las copias de seguridad es una actividad ejecutada de forma notable por las empresas. No obstante y como se indicaba anteriormente, la forma de llevarlas a cabo no permite concluir que sean efectivas, puesto que tan importante como realizar las copias es comprobar la recuperación efectiva de la información, custodiar las copias en una ubicación distinta o garantizar la restricción del acceso a las mismas a determinados empleados. Estos procedimientos no son observados uniformemente por la totalidad del colectivo entrevistado y están condicionados en gran medida por su tamaño.

4.2 ACTUALIZACIÓN DE PROGRAMAS Y SISTEMAS

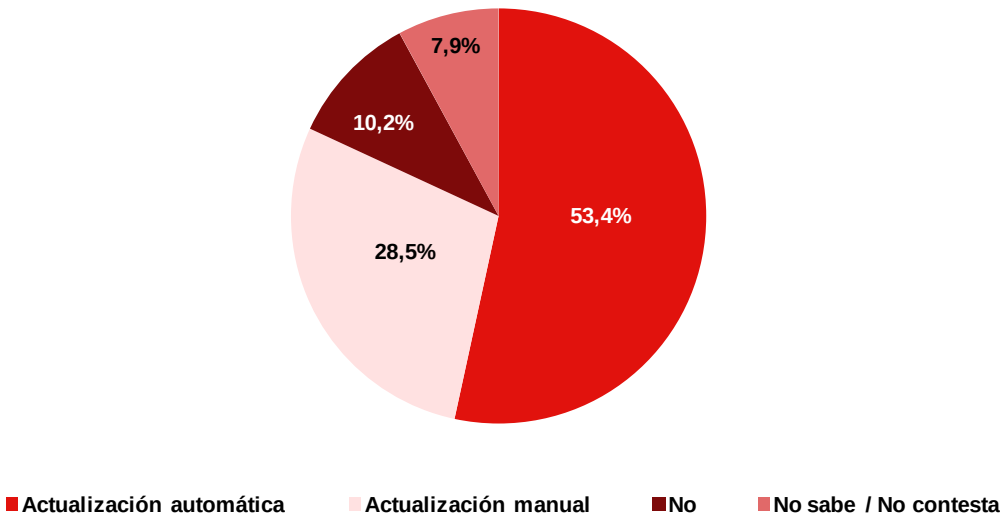
Las amenazas evolucionan constantemente, y los equipos informáticos deben estar protegidos para hacer frente a ellas. Una buena práctica de seguridad es el mantenimiento de las actualizaciones del sistema operativo y programas informáticos, puesto que permiten evitar defectos en la programación y por tanto, vulnerabilidades frente a posibles ataques. Por tanto se estudia en el presente epígrafe el grado de preparación de las empresas para realizar un correcto mantenimiento y actualización de los equipos y programas.

En general, las empresas parecen estar al tanto de los beneficios que aporta la actualización de programas y sistemas, puesto que un elevado porcentaje indica realizarlas, un 81,9%.

La actualización de los programas y sistemas puede hacerse principalmente a través de dos modalidades: de forma automática o manual. Como muestra el siguiente gráfico, un 53,4% de organizaciones se decantan por mecanismos automáticos, mientras que un 28,5% realiza las actualizaciones de forma manual.

No existen diferencias destacadas en el análisis por tamaño de empresa.

Gráfico 19: Realización de actualizaciones del sistema operativo y programas (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

En general, se desprende de los datos que las empresas adoptan una posición pasiva frente a las actualizaciones del sistema operativo y de los programas, confiando en las que realiza de forma automática el propio sistema. En opinión de los expertos que han participado en el estudio, este aspecto denota un desconocimiento de los procedimientos para llevar a cabo las actualizaciones. Este motivo puede estar detrás del hábito declarado por los responsables de seguridad entrevistados, quienes afirman que *"desconfían de las actualizaciones en el momento de su ubicación y esperan a que otros lo hayan probado, puesto que no saben lo que conllevan."*

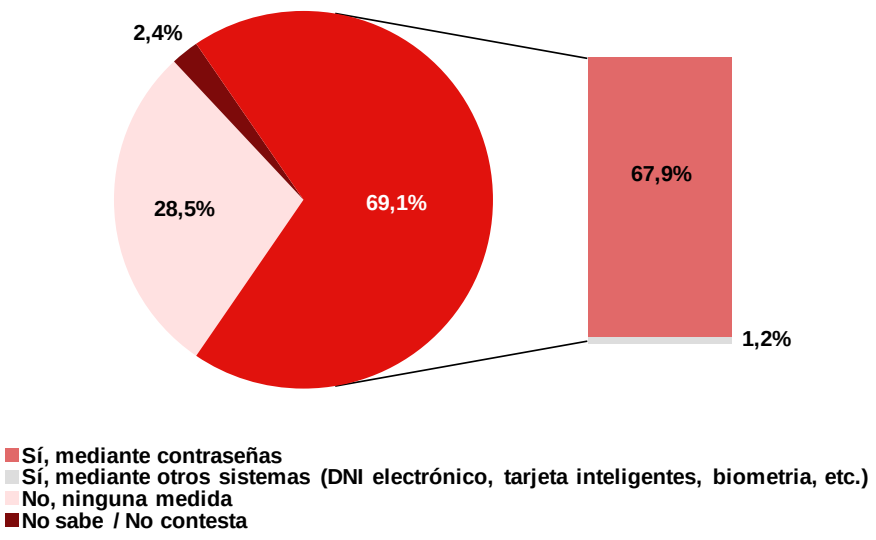
4.3 MEDIDAS DE CONTROL DE ACCESO A EQUIPOS Y DOCUMENTOS

El control de acceso a equipos y documentos es un conjunto de protocolos necesarios que permite la entrada restringida a áreas específicas para determinados grupos de trabajo o personas. Supone una barrera inmediata que define los permisos de circulación y acceso al personal, para la que se pueden utilizar diversas herramientas: contraseñas, DNI electrónico, tarjeta inteligente, biometría, etc. Este control permite aumentar la seguridad de la información en la empresa, al disminuir sensiblemente las posibilidades de intrusión de terceras personas.

En el siguiente gráfico se muestra que casi 7 de cada 10 empresas participantes en el estudio tienen instaladas medidas de control de acceso a equipos y documentos, fundamentalmente contraseñas (declarada por un 67,9% frente a un 1,2% que se decanta por otros sistemas). Un 28,5% que no dispone de controles.

Se observa una relación directa entre el tamaño de la empresa y el nivel de adopción de medidas de seguridad: en las compañías de 50 a 250 trabajadores el control en el acceso a los equipos está totalmente extendido, mientras que en las que tienen menos de diez trabajadores aún existe un porcentaje relevante que no observa ninguna precaución.

Gráfico 20: Medidas de control de acceso a equipos y documentos (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

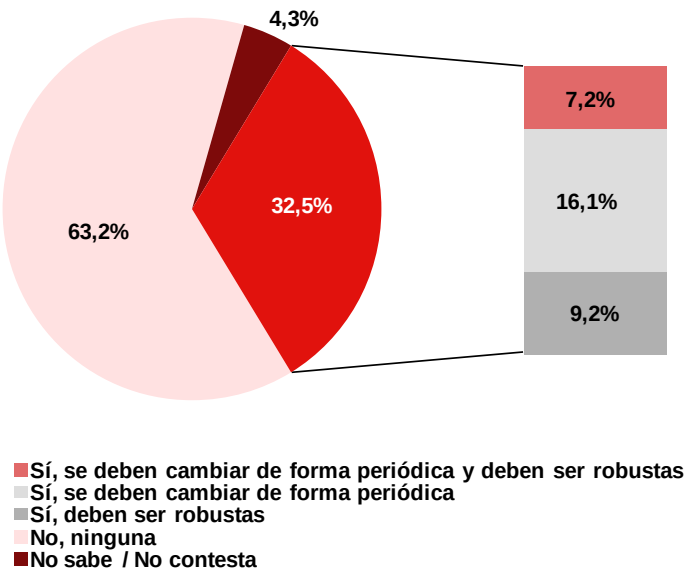
Junto con la existencia de contraseñas, es importante analizar las medidas que establece la empresa para que estas sean eficaces y proporcionen el nivel de seguridad esperado. Así, se recomienda que las contraseñas sean robustas y que se cambien con cierta frecuencia.

En la práctica, 1 de cada 3 empresas han adoptado normas para la creación de contraseñas: un 9,2% declaran haber establecido el criterio de la robustez, el 16,1% de la periodicidad con la que deben ser renovadas las claves y un 7,2% imponen ambos criterios.

Por el contrario, un 63,2% de las empresas no han establecido normas para la gestión de las contraseñas, lo que indica que todavía queda trabajo por hacer en este sentido.

Al igual que ocurría en el caso anterior, las empresas de mayor tamaño desarrollan procedimientos para esta actividad (abarcando criterios de robustez y periodicidad), mientras que en las micro y pequeñas empresas son más frecuentes los relativos a la periodicidad.

Gráfico 21: Existencia de normas para la creación de contraseñas (%)



Base: Empresas que utilizan contraseñas (n=939) *Fuente: INTECO*

Por lo tanto, a pesar de que 2 de cada 3 empresas han establecido contraseñas para el control de acceso a equipos y documentos a determinadas personas, no están igualmente extendidas las normas para su creación y mantenimiento. Como indican los expertos y los responsables de seguridad de las empresas entrevistadas, es necesario seguir mejorando en la sensibilización respecto a los controles de acceso y los criterios necesarios para que sean efectivos y permitan garantizar la seguridad de la información.

4.4 BUENAS PRÁCTICAS EN DISPOSITIVOS MÓVILES

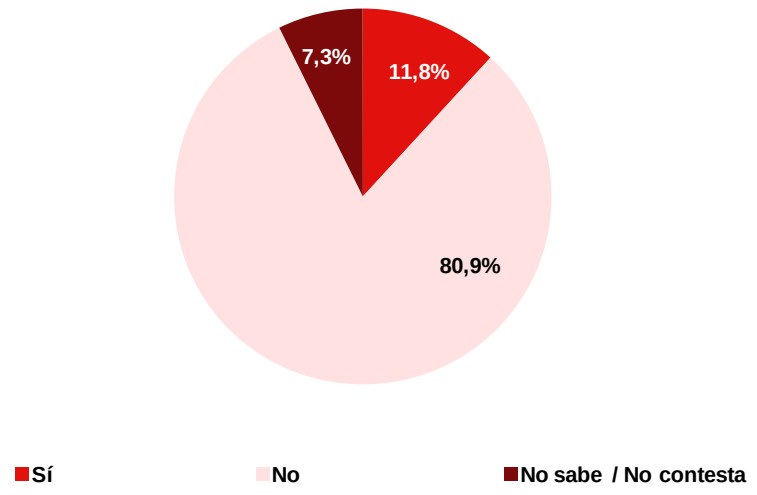
La importancia creciente de la utilización de dispositivos móviles como herramienta de trabajo implica la necesidad de mayores garantías de seguridad. Por ello, se analiza la existencia de políticas de uso seguro dirigidas a los empleados que utilizan estas tecnologías, puesto que la

disposición de unas directrices por parte del usuario permite optimizar el rendimiento de los terminales y evitar situaciones no deseadas como fraudes y pérdida de información.

De las empresas que afirman tener dispositivos móviles, ocho de cada diez declara que no cuenta con una política de este tipo (80,9%), frente a un 11,8% que afirma que sí dispone de ella.

Cuanto mayor es el tamaño de la empresa, mayor posibilidad hay de que existan normas de uso de los teléfonos inteligentes, tabletas y PDAs: en las medianas empresas esta proporción alcanza el 30,8%, mientras que en la microempresa, desciende hasta un 10,8%.

Gráfico 22: Disponibilidad de política de uso seguro de dispositivos móviles (smartphones, PDAs, tabletas, etc.) (%)



Base: Empresas que tienen dispositivos móviles (n=459) *Fuente: INTECO*

4.5 BUENAS PRÁCTICAS PARA LOS EMPLEADOS

Además de disponer de los recursos técnicos destinados a la seguridad de la información, es imprescindible que los empleados realicen una buena gestión de ellos. Así, las empresas pueden establecer diferentes limitaciones de acceso a servicios y contenidos de Internet, bien con carácter general, bien para determinados servicios y/o perfiles. Por ello es importante definir un conjunto de buenas prácticas que promuevan un uso seguro y responsable de los servicios relacionados con las tecnologías de la información y las comunicaciones.

En el presente apartado se analizan las limitaciones que la empresa impone a sus empleados para el acceso a los contenidos de Internet, la capacidad de estos para instalar programas, y la formación específica que la empresa les proporciona.

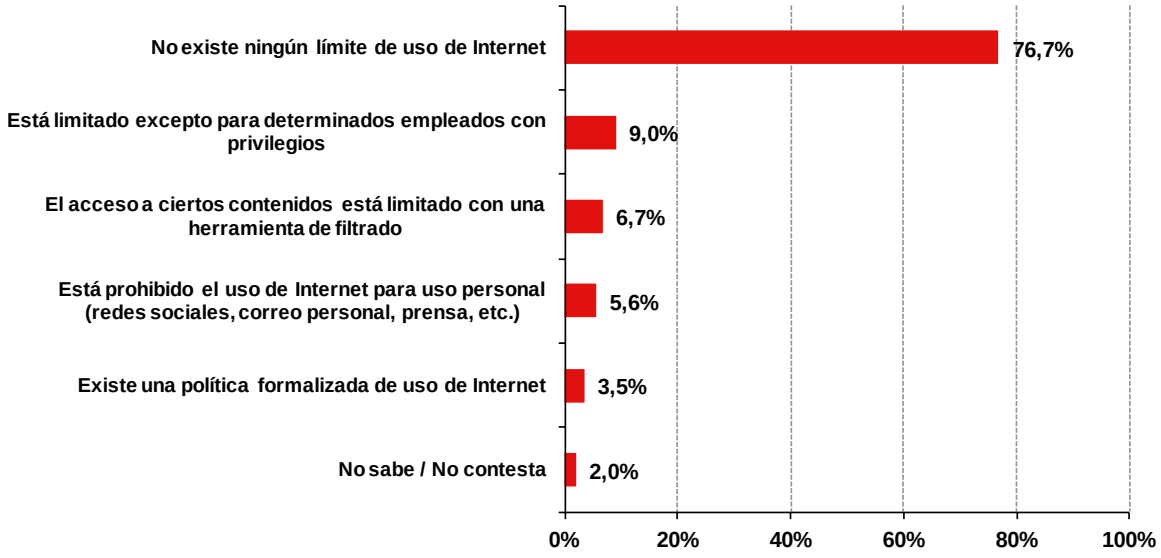
En primer lugar, las empresas establecen diferentes controles para el acceso a Internet por parte de sus empleados: un 9% gestiona este acceso centralizándolo en unos pocos empleados a los que concede privilegios, un 6,7% realiza este filtro a través de herramientas de filtrado en el

navegador. Por su parte, un 5,6% de las empresas prohíben el uso de servicios de tipo personal (redes sociales, correo personal, etc.). Por último, un 3,5% afirman proporcionar a los empleados una orientación común para el uso de Internet.

A pesar de tener en cuenta diversas posibilidades, esta práctica es reducida: un 76,7% de las empresas afirma no tener ninguna limitación de acceso.

El análisis más pormenorizado y segmentado en función del tamaño indica la relación inversa entre el tamaño y la libertad de acceso de los empleados a la Red. Asimismo, la presencia de limitaciones en el acceso a los servicios y contenidos de Internet es heterogénea en función del tipo de empresa: así, mientras micro y pequeñas empresas optan por un control gestionado por responsables, las medianas disponen en mayor medida de herramientas y procedimientos. Por otra parte, pequeñas y medianas conceden la menor importancia a la limitación de Internet para uso personal.

Gráfico 23: Existencia de límites de acceso a los servicios y contenidos de Internet para los empleados (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

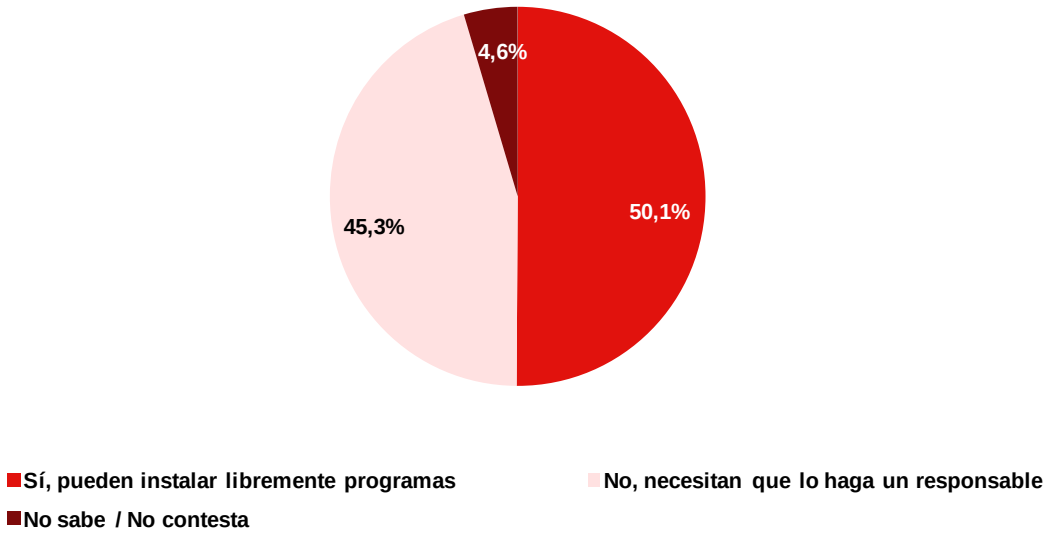
El segundo lugar, se analiza el hábito prudente relativo a la concesión de permisos para la instalación de programas. La instalación o incorporación en el equipo de aplicaciones y dispositivos es un proceso que no está exento de riesgos de seguridad (infección por malware, vulnerabilidades relacionadas con la descarga e instalación de software, etc.) si no se toman las precauciones necesarias.

Los expertos recomiendan que esta práctica sea realizada por personal cualificado para ello, por ejemplo un profesional informático, en caso de que exista esa figura. En este sentido, es importante estudiar si se supervisa el proceso de instalación en la empresa, es decir, si se extiende la seguridad a aspectos organizativos.

Como muestra el Gráfico 24, la mitad de las organizaciones participantes en el estudio dicen dar libertad a sus trabajadores para instalar programas, mientras que un 45,3% afirma contar con una figura que se encarga de gestionar esta actividad.

En la pequeña y mediana empresa existe un comportamiento similar: ambos grupos señalan en gran medida que la instalación de los programas necesita ser ejecutada por un responsable (un 72,3% y un 79,8% respectivamente), mientras que la microempresa sólo dispone de esta figura en un 43,6% de los casos. Esta circunstancia se debe en parte a que las empresas más pequeñas, carecen de un responsable de informática que lleve a cabo la instalación y el control de los programas, de modo que son los propios trabajadores los que se encargan de esta tarea. Por otro lado, en este estrato el reducido número de trabajadores implica que los empleados que realizan otras tareas asuman también las relacionadas con la informática y la seguridad de la información.

Gráfico 24: Percepción de la capacidad de los empleados para instalar programas (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

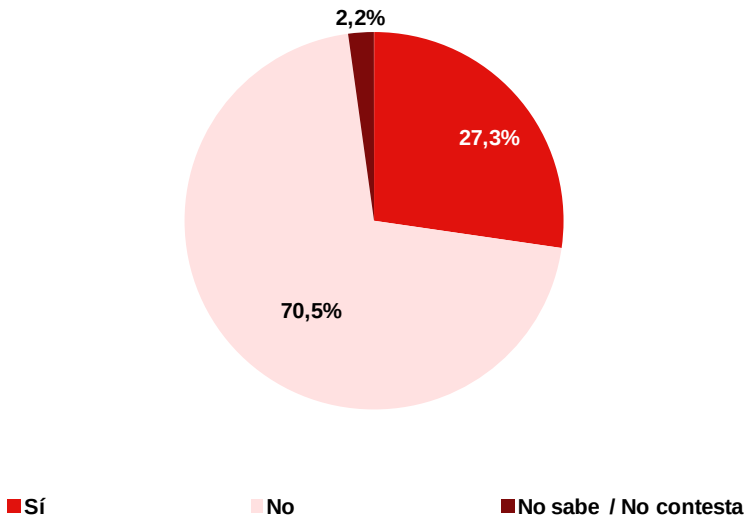
Por último, con el objeto de mantener y mejorar la seguridad de la información de las empresas, además de disponer de personal dedicado a ello es necesario que los trabajadores tengan conocimiento de cuestiones básicas de seguridad. En este sentido, el porcentaje de empresas que facilitan formación específica sobre los riesgos en seguridad alcanza el 27,3%.

Según el estudio “Tecnologías de la información y la comunicación en la empresa”, realizado por AETIC-Everis en el año 2011, el 14,0% de las empresas realiza habitualmente formación específica en TIC / uso de la informática, el 39,0% lo hace alguna vez, mientras que el 46,4% no lo realiza nunca. Al comparar ambos estudios, se advierte que los datos obtenidos por INTECO se sitúan en un valor intermedio del estudio AETIC-Everis, entre quienes se le informa habitualmente y quienes lo hacen alguna vez (teniendo en cuenta que dentro de esta formación, se pueden proporcionar nociones de seguridad).

Por su parte, los expertos consultados en el marco del estudio consideran que la formación declarada por las empresas sobre riesgos de seguridad adquiere valores muy altos y que, en realidad, el porcentaje es sensiblemente menor. Así mismo, consideran necesario mejorar la sensibilización en la organización, promoviendo acciones informativas y formativas en aspectos de seguridad. A este respecto, los responsables de las empresas participantes en las entrevistas en profundidad añaden el excesivo coste de la formación específica en materia de seguridad, por lo que *"sería deseable que esta fuera subvencionada o financiada y que desde la Administración se promovieran acciones específicas de concienciación".*

Para concluir, el análisis atendiendo al sector en el que opera la empresa indica que esta práctica es más probable en empresas relacionadas con el sector TIC y de servicios a empresas, mientras que se da con menor frecuencia en sectores como el de logística y comunicaciones, industria o comercio.

Gráfico 25: Formación específica sobre riesgos de seguridad en las empresas (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

5 PLANES Y POLÍTICAS DE SEGURIDAD

La disposición de planes y políticas de seguridad por parte de las empresas es otra de las prácticas que les permiten disponer de una estrategia para el aumento progresivo del nivel de seguridad.

En el siguiente apartado se analiza, entre otras cuestiones, la percepción de la compañía sobre planes y políticas de seguridad, el análisis del conocimiento sobre los planes de continuidad de negocio, y la situación de la seguridad desde el punto de vista de la continuidad, así como sus estrategias y procedimientos.

5.1 PERCEPCIÓN DE LA EMPRESA SOBRE PLANES Y POLÍTICAS DE SEGURIDAD

Un mecanismo importante para el mantenimiento e incremento de la protección de la información en las empresas es el desarrollo de planes y políticas de seguridad.

La percepción en cuanto a la realización de auditorías de seguridad sirve como primer indicador del establecimiento de mecanismos que permitan evaluar la situación de seguridad en la empresa y establecer actuaciones de mejora. Esta medida constituye una obligación para aquellas empresas con ficheros de datos con un nivel de seguridad medio o superior.

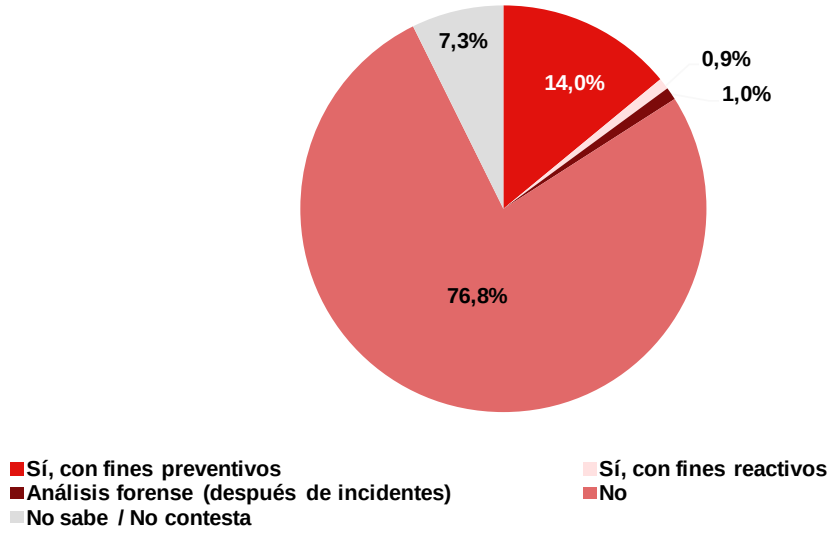
En este sentido, el 15,9% de las empresas afirma llevar a cabo auditorías de seguridad, en gran parte como medida de prevención (14%) y de forma minoritaria con carácter reactivo (0,9%) o de análisis forense tras un incidente (1%).

Las empresas participantes en las entrevistas de seguridad son conscientes de que es una medida deseable, aunque depende mucho de los recursos de la empresa y del grado de compromiso de la dirección. Los expertos señalan que *"en realidad es una práctica con un nivel de ejecución muy inferior a la percibida por las pequeñas y medianas empresas"*, puesto que existe cierta confusión con respecto al concepto de auditoría.

Los motivos que apuntan estos profesionales son diversos: en primer lugar, los escaneos de seguridad realizados por las soluciones antivirus en muchos casos son percibidos por las empresas como auditorias de seguridad, por lo que incluso aquellas organizaciones con ficheros que contienen datos de nivel bajo (y por tanto, sin obligación de realizar auditoría de seguridad) responden afirmativamente a esta cuestión. Otra posible explicación estaría en el hecho de que más de un tercio de las empresas externalizan la gestión de la seguridad, por lo que pueden percibir que realizan auditorias. Por ello, los expertos proponen que desde las administraciones públicas *"se realicen campañas de concienciación para las empresas en materia de políticas y requerimientos de seguridad".*

Como ocurre en casos anteriores, existe una relación directa entre el mayor tamaño de la empresa y la realización de esta medida. Así, un 55,4% las empresas de mayor tamaño afirman llevar a cabo auditorías, proporción muy superior al dato global.

Gráfico 26: Percepción de la realización de auditorías de seguridad en la empresa (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

La forma más idónea para garantizar la incorporación de planes y políticas de seguridad es la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este estándar está construido en base a la norma ISO 27001, que especifica los requisitos necesarios para establecer, implantar y mejorar la gestión de la seguridad de la información en cualquier organización. Entre otras cuestiones tiene el propósito de garantizar que los riesgos de seguridad sean conocidos y gestionados por la organización, y se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

La implantación de un SGSI obliga a tener en cuenta una visión global sobre el estado de seguridad de los sistemas de información, hecho considerado como el primer paso para afrontar con posterioridad una estrategia de continuidad de negocio.

Asimismo, como señalan los expertos, la certificación permite a las organizaciones proporcionar unas garantías de cumplimiento respecto a los servicios ofrecidos a sus clientes y colaboradores.

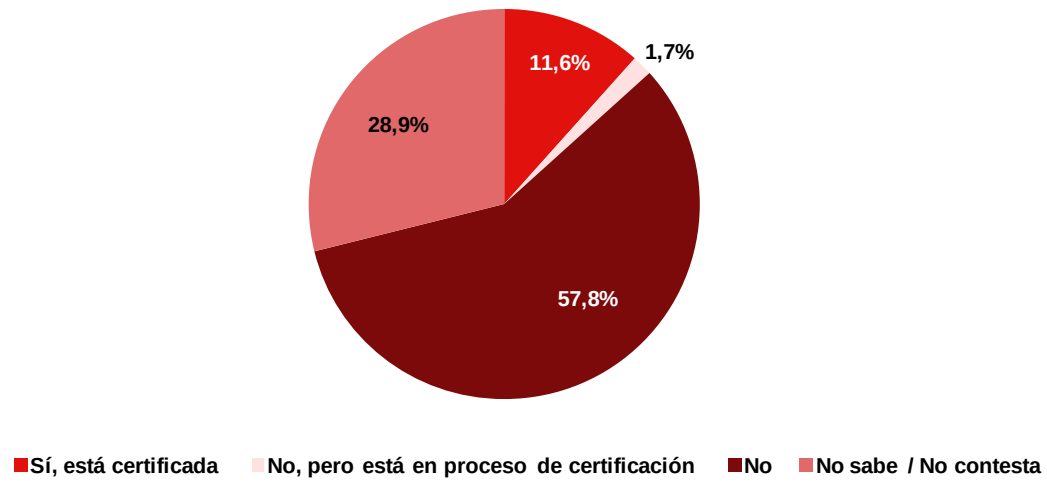
En el momento de realización de la encuesta, un 13,3% de las empresas afirma estar certificada o en proceso de certificación en la gestión de la seguridad de la información. Destaca también que un 28,9% no se manifiesta al respecto, revelando un cierto desconocimiento.

En este sentido, los expertos consultados indican que *"la proporción real es menor",* y consideran que existe una confusión entre la ISO 27001 y otras normas más comunes en la empresa, como la ISO 9001 relativa a sistemas de gestión de la calidad en la empresa.

El análisis documental clarifica que en 2010 existían en España 711 empresas certificadas en 27001 sobre sistemas de gestión de la seguridad de la información[21], lo que supone un 0,02% sobre el total de empresas existentes en España.

INTECO ha contribuido a dinamizar el mercado de la implantación y certificación en SGSI. Así, en 2009 llevó a cabo el Programa de impulso a la implantación y certificación de Sistemas de Gestión de Seguridad de la Información, SGSI (ISO 27001) en la PYME española, en el que se certificaron 143 pequeñas y medianas empresas, logrando posicionar a España entre los países del mundo con más implantaciones de ISO 27001.

Gráfico 27: Empresas que declaran estar certificadas en ISO 27001 sobre Sistemas de Gestión de la Seguridad de la Información o SGSI (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

5.2 ANÁLISIS DEL CONOCIMIENTO SOBRE MEDIDAS O PLANES DE CONTINUIDAD DE NEGOCIO

Junto con el nivel de implantación de medidas de seguridad que las empresas afirman disponer, es interesante analizar el grado de conocimiento en el ámbito de la seguridad orientada a garantizar la continuidad de las operaciones en caso de desastre.

Un Plan de Continuidad de Negocio (PCN) es el conjunto de medidas, procesos de actuación y responsables que garantizan el restablecimiento de las operaciones críticas de negocio en el menor tiempo posible tras padecer una crisis/desastre.

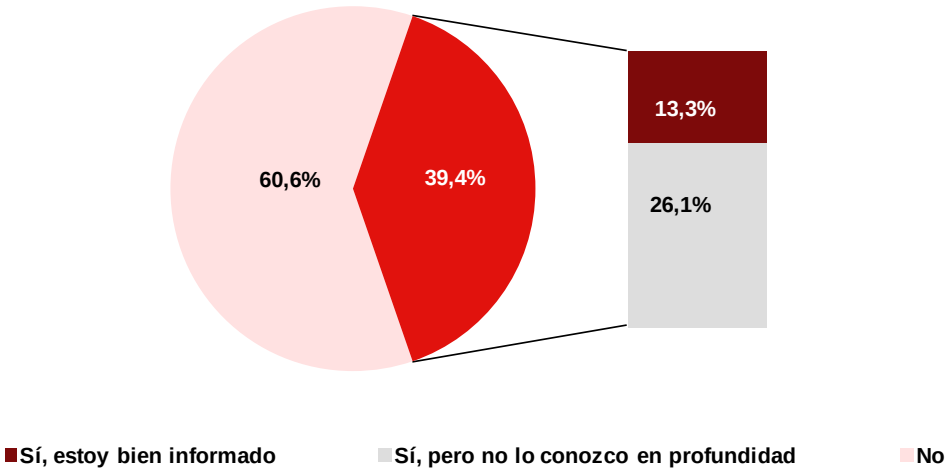
[21] Fuente: International Organization for Standardization (ISO) (2011) *The ISO Survey of Certifications 2010*. Disponible en: http://www.iso.org/iso/iso-survey2010.pdf

En líneas generales se advierte que existe, por parte de las empresas encuestadas, un desconocimiento importante del concepto y utilidad del Plan de Continuidad de Negocio: seis de cada diez afirman que no lo conocen.

Frente a este desconocimiento, un 13,3% creen que están bien informados y un 26,1% no lo conoce en profundidad.

Esta cultura es heterogénea en función del sector de actividad de la empresa: las empresas que operan como proveedores de otras empresas (servicios empresariales) y del sector relacionado con las nuevas tecnologías de la información y las comunicaciones (Informática, I+D+i y telecomunicaciones) son las que señalan estar más familiarizadas con estos conceptos, mientras que las del sector industria y construcción indican que están informadas aunque no de forma detallada.

Gráfico 28: Conocimiento de lo que es un Plan de Continuidad de Negocio (%)

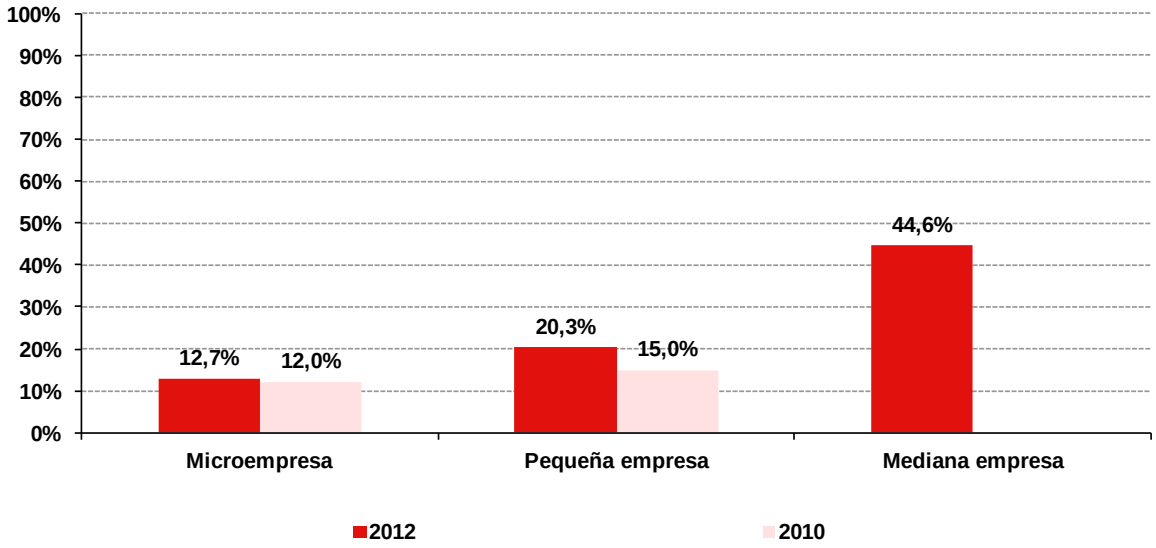


Base: Total empresas que responden a la parte de continuidad de negocio (CN) n=1.109 *Fuente: INTECO*

El análisis longitudinal por tamaño de empresa muestra –además de la relación directa entre tamaño y mayor conocimiento– un aumento del saber en materia de PCN con respecto a 2010, especialmente en la pequeña empresa[22].

[22] No se tienen datos comparativos con respecto a la mediana empresa puesto que en el estudio realizado en el 2010 este estrato no formó parte de la muestra.

Gráfico 29 : Evolución del grado de conocimiento "bueno" del PCN según tamaño (%)



Base: Total empresas que responden a la parte de CN n=1.109 *Fuente: INTECO*

Se puede concluir que existe un tímido interés y sensibilidad en la pequeña y mediana empresa española por los aspectos relacionados con la continuidad de negocio y de la relación de esta planificación con el adecuado funcionamiento de la organización. Esto denota una falta de planificación ante los posibles eventos adversos que harían peligrar el negocio, de producirse.

No obstante, se advierte una tendencia positiva en los últimos años y los expertos que han formado parte del estudio consideran que el porcentaje de empresas que realmente conocen el PCN es mayor, aunque desconocen esta terminología. Es decir, las empresas conocen en mayor o menor medida cuáles son las actividades críticas de su negocio y las medidas a seguir en caso de situación de crisis. No obstante puede que estas directrices no estén recogidas en un Plan.

5.3 SITUACIÓN DE SEGURIDAD DE LA EMPRESA ESPAÑOLA DESDE EL PUNTO DE VISTA DE LA CONTINUIDAD DE NEGOCIO

"La adopción de una estrategia de continuidad constituye un ejercicio de responsabilidad y predisposición a anticiparse a cualquier tipo de elemento adverso que haga peligrar el negocio"[23].

Esto es así puesto que, junto a situaciones más esporádicas como las catástrofes, se producen incidentes más frecuentes pero de menor repercusión que, de no ser gestionados convenientemente, pueden desencadenar en un problema mayor. Estos incidentes vienen a recordar la necesidad contemplar la gestión de la continuidad de negocio en los procesos integrales de gestión de riesgos de las empresas, independientemente de su tamaño o sector.

La Gestión de la Continuidad de Negocio abarca una serie de actividades:

[23] Fuente: INTECO (2010). *Guía práctica para PYMES: cómo implantar un PCN*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/guias/guia_continuidad

- **Fase I – Diseño del Plan y establecimiento de la Política de Continuidad de Negocio**: comprende la identificación de las actividades que deben ser realizadas de forma previa para comenzar el proceso de desarrollo e implantación del Plan de Continuidad.

- **Fase II – Conocimiento de los procesos de negocio de la organización y análisis de riesgos** que impactan en las actividades de negocio: con el fin de identificar los productos y servicios clave de la empresa, los recursos clave que soportan estas actividades y los riesgos a los que está expuesta.

- **Fase III – Medidas preventivas**: esta fase plantea la posibilidad de aplicar medidas de seguridad preventivas y proactivas con la intención, en la medida de lo posible, de evitar o gestionar los incidentes graves, sin necesidad de activar el plan de continuidad de negocio a no ser que sea estrictamente necesario.

- **Fase IV – Estrategia de recuperación**: considerando que no todas las actividades de negocio tienen las mismas prioridades de recuperación, esta fase establece los objetivos y las prioridades de recuperación en función de los riesgos que impactan en las operaciones de negocio.

- **Fase V – Desarrollo e implantación del Plan**: conjunto de prácticas, procedimientos a seguir y tecnologías para la recuperación de las operaciones críticas después de producirse un desastre. Dichos procedimientos deben soportar las estrategias de recuperación previamente seleccionadas.

- **Fase VI – Mantenimiento del Plan:** teniendo en cuenta que todo Plan de Continuidad de Negocio debe ser difundido, revisado, actualizado y probado regularmente, esta fase describe acciones de difusión y formación del Plan, así como las pruebas y el proceso de mejora continua del mismo.

De cara a establecer un diagnóstico sobre la situación actual en la pequeña y mediana empresa de la gestión de la continuidad del negocio, se analizan diferentes etapas o hitos en este proceso.

5.3.1 Diseño y establecimiento de estrategias de continuidad de negocio

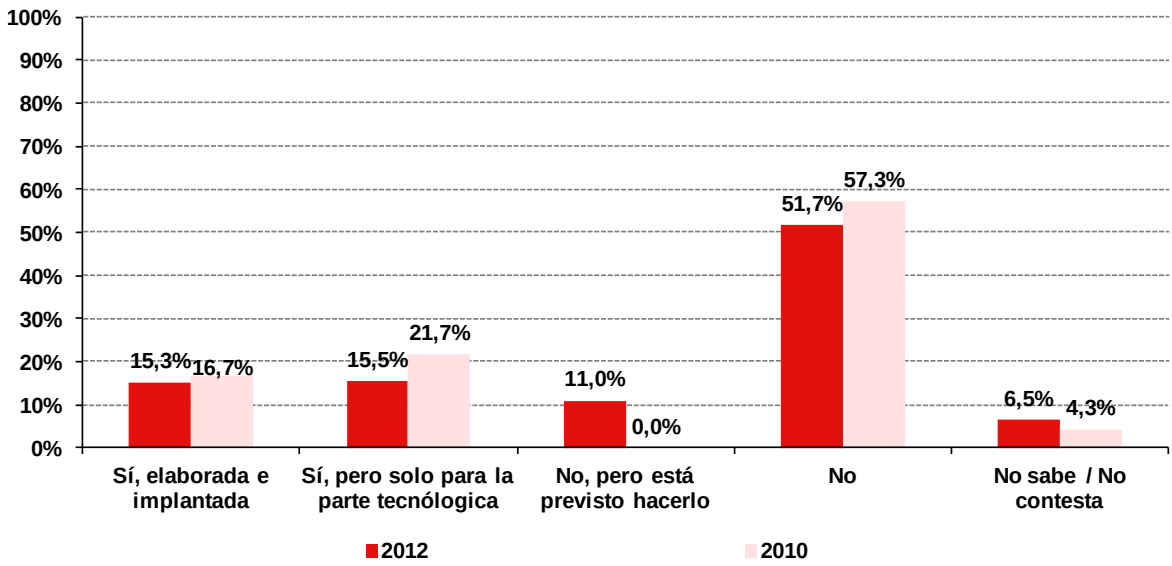
En primer lugar, el colectivo participante en el estudio indica la disposición de estrategias internas que garanticen la resistencia de la organización ante cualquier suceso que pueda poner en peligro su supervivencia.

Así, un 30,8% de las empresas tienen implantada alguna estrategia o procedimiento en caso de situaciones de crisis o desastre, bien refiriéndose a una estrategia completa (15,3%), bien relativo a mecanismos para la recuperación exclusivamente del entorno tecnológico que soporta las operaciones de negocio (15,5%). Además, un 11,0% indica que no tiene implantada ninguna estrategia pero que tiene previsto hacerlo.

El sector al que pertenece la empresa influye en el tipo de estrategia adoptada. En este sentido, la probabilidad de que las empresas relativas a la actividad de servicios dispongan de estrategias completas de continuidad de negocio es mayor que en el resto de sectores. En el caso de la disposición de procedimientos que se ocupan de la parte tecnológica, es el sector de nuevas tecnologías el que presenta mejores ratios de implementación. Por último, el sector de hostelería y comercio muestra mayor predisposición por incluir estas estrategias en el futuro.

La evolución experimentada en los valores desde 2010 es bastante estable, destacando la proporción de empresas que en 2012 indican que tienen previsto incorporar una estrategia (opción declarada por un 11,0% en 2012 y no utilizada en 2010).

Gráfico 30: Evolución de la previsión de alguna estrategia o procedimiento en caso de situaciones de crisis/desastre que afecten al negocio (%)



Base 2012: total de empresas (n=1.109) *Fuente: INTECO*
Base 2010: total de empresas (n=400)

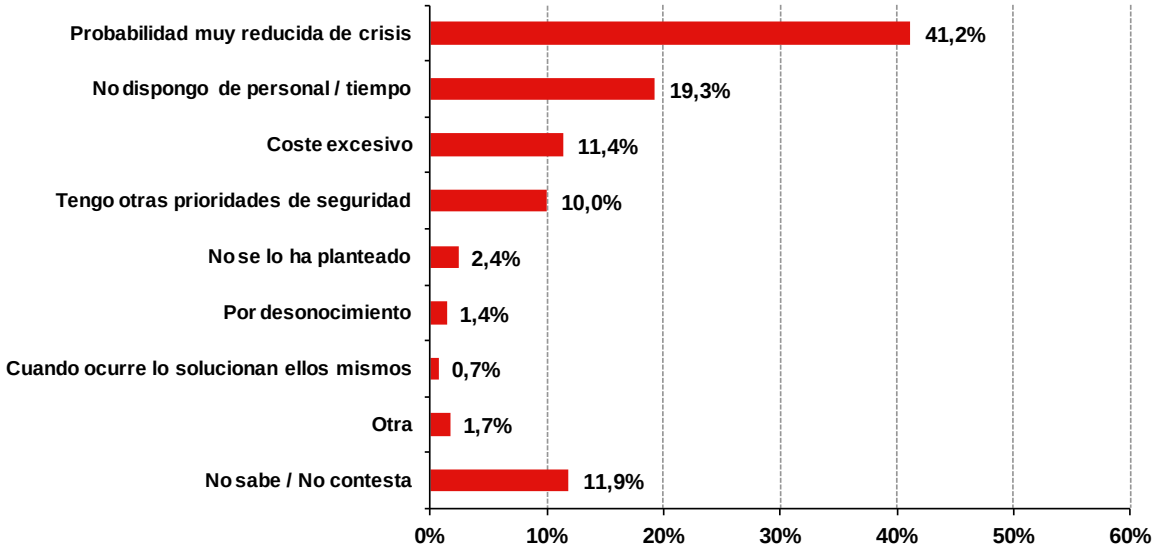
El análisis de los motivos que las organizaciones alegan para no disponer de sistemas que permitan hacer frente a contingencias graves proporciona las siguientes conclusiones:

- Por un lado, es notable el porcentaje de empresas que no están concienciadas de la necesidad crítica de disponer de medidas de respuesta frente a determinados acontecimientos. Así, un 41,2% señala que la probabilidad de que se produzca el incidente es muy reducida y que, por lo tanto, no priorizan esta medida. Al mismo tiempo, un 10% alega que estas medidas no están entre las preferencias de seguridad.

- Por otro lado, un 30,7% indica que no cuenta con recursos suficientes para abordar esta cuestión. A juicio de un 11,4%, el coste de implantar este tipo de estrategias es muy elevado, mientras que para un 19,3% adicional, no disponen de personal ni tiempo como para abordar la implantación de una estrategia de continuidad de negocio.

Las conclusiones obtenidas por Deloitte[24] son similares a las del presente estudio. Entre las razones que alega las entidades que no ha optado por definir una política o estrategia que permita mantener sus actividades de negocio, se encuentran fundamentalmente el considerar muy reducida la probabilidad de ocurrencia de una crisis o desastre (49,1%), no disponer de presupuesto suficiente (15,1%) o considerar que el coste de implantación supone un gasto innecesario (11,3%).

Gráfico 31: Razón por la que no se ha previsto una estrategia o procedimiento ante situaciones de crisis o desastre (%)



Base: Empresas que carecen de estrategia de CN (n=416) *Fuente: INTECO*

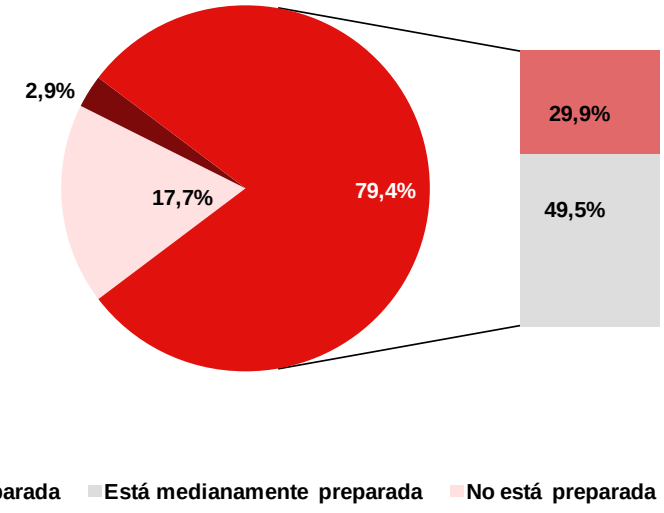
El hecho de que todavía muchas empresas no dispongan de una estrategia no parece influir en la percepción que tienen de estar preparadas para afrontar una situación de desastre, crisis o contingencia. Un 79,4% de empresas así lo afirman, si bien sólo tres de cada diez creen que esta preparación sea buena.

Los expertos creen que esa percepción dista mucho de la realidad, porque en su opinión es reducido el número de empresas que podrían hacer frente a una paralización, como confirman los resultados respecto a identificación de las actividades críticas del negocio, la tenencia de una estrategia para situaciones de crisis y los datos de implementación de medidas o planes de recuperación ante desastres. De todo ello, concluyen que existe una falsa percepción de seguridad.

[24] Fuente: DELOITTE (2010). *Valoración del primer semestre de 2010 y previsiones para el segundo semestre de 2010. Planes de Continuidad de Negocio. Disponible en:* http://www.deloitte.com/assets/Dcom-Spain/Local%20Assets/Documents/Barometro%20de%20Empresas/es_barometro_empresas_36.pdf

Teniendo en cuenta el tipo de empresa (microempresa, pequeña o mediana empresa), esta preparación es más elevada en las empresas de mayor tamaño, mientras que en las micro y pequeñas empresas es más frecuente que indiquen estar medianamente capacitadas.

Gráfico 32: Posición afirmada por la empresa para afrontar una situación de crisis, desastre o contingencia (%)



Base: Total empresas que responden a la parte de CN (n=1.109) *Fuente: INTECO*

5.3.2 Estudio de los procesos de negocio e identificación de actividades críticas

Un segundo aspecto relevante en la gestión de la continuidad es el estudio de las actividades de negocio en cuanto a los activos o recursos de que dispone y las interrelaciones existentes entre ellos. A partir de este estudio, las empresas deben identificar las actividades críticas, es decir, aquellas cuyo fallo o interrupción impactaría en sus relaciones de negocio y comerciales, en sus ingresos o en su imagen.

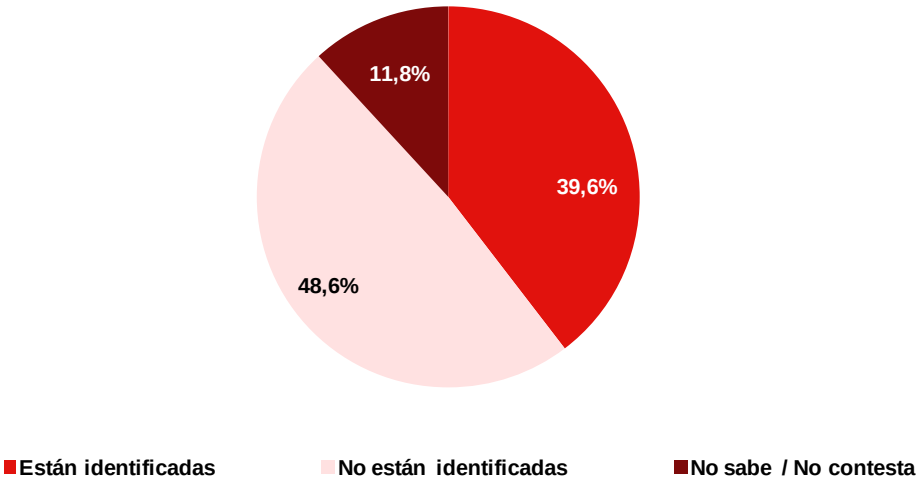
La identificación de las actividades críticas permite responder más rápidamente y de forma más preparada ante cualquier tipo de incidencia, es decir, facilita la restauración de aquellas actividades que, siendo vitales para el funcionamiento de la empresa, son paralizadas tras un desastre o contingencia.

Según las respuestas aportadas, un 39,6% afirma haber identificado sus operaciones críticas de negocio, frente a un 48,6% que indican no tenerlas recogidas. Igualmente es destacable que un 11,8% de las empresas desconocen si están identificadas o no.

Las microempresas y pequeñas empresas son las que identifican en menor proporción las actividades críticas de negocio. En función del sector económico, existe una mayor probabilidad de tener recogidas las críticas en las empresas de nuevas tecnologías, servicios empresariales y transporte. Por el contrario, en los sectores industriales y de comercio y hostelería, hay una menor proporción de empresas que señalan conocer estas operaciones.

Según los propios responsables de seguridad, *"la empresa vive el día a día y no son conscientes del impacto que podría tener un suceso crítico"*. Asimismo, destacan la necesidad de formar a los directivos, que en muchos casos no tienen un perfil profesional de gestión y desconocen los aspectos relacionados con la seguridad de la información y CN.

Gráfico 33: Grado de identificación percibido de las operaciones críticas de negocio (%)

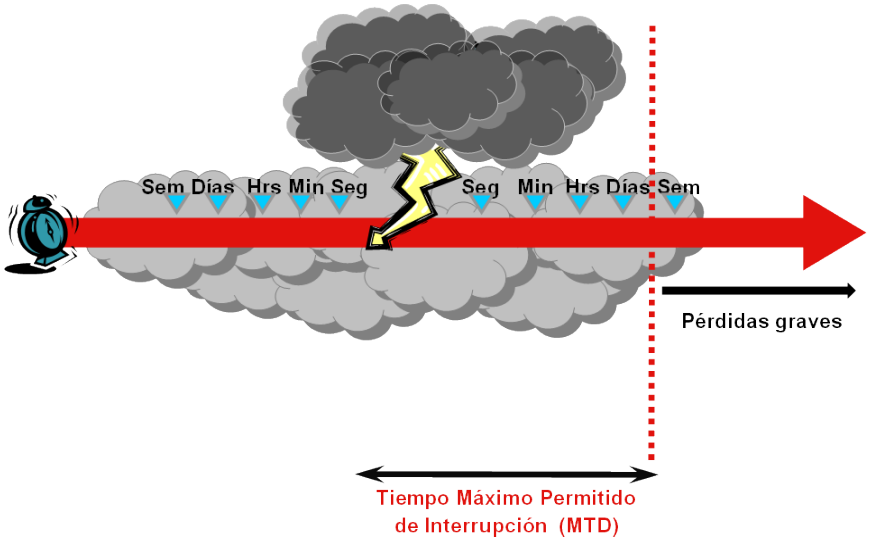


Base: Total empresas que responden a la parte de CN (n=1.109) *Fuente: INTECO*

5.3.3 Valoración del impacto asociado a la interrupción de la actividad

Junto con la identificación de las actividades y recursos críticos del negocio, las empresas deben valorar el impacto que produciría una paralización de las actividades, así como el tiempo de interrupción que podría soportarse desde que se produce el desastre hasta que las pérdidas no fueran asumibles.

Ilustración 3: Línea temporal hasta el tiempo máximo permitido de interrupción



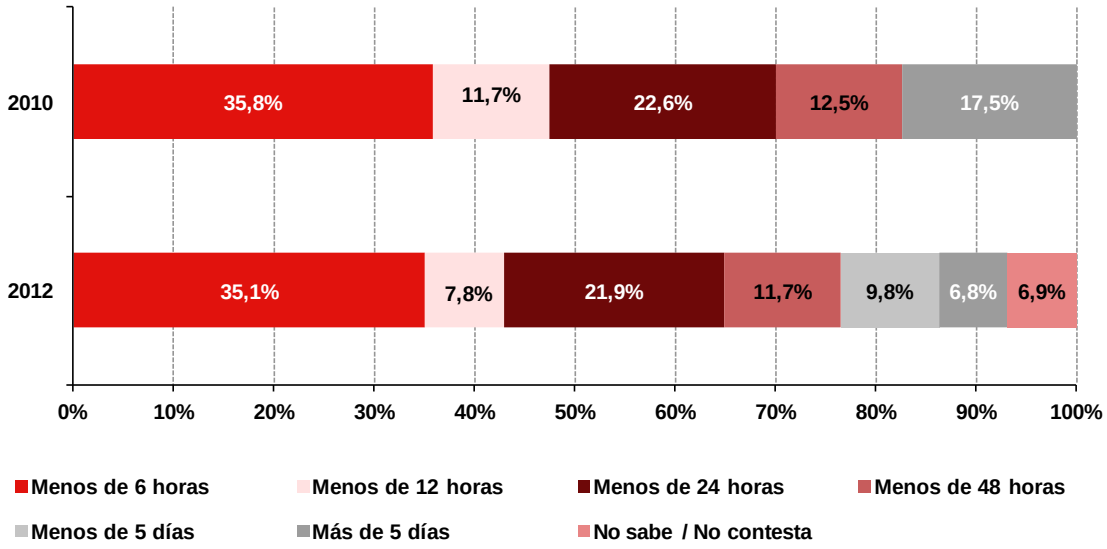
Fuente: INTECO

A la hora de identificar el tiempo máximo durante el que las actividades principales de negocio podrían estar interrumpidas a causa de un incidente o contingencia grave, un 35,1% de las empresas consultadas señalan que este periodo no puede ser superior a 6 horas, mientras que un 21,9% ha señalado que del límite está en 24 horas.

Los resultados obtenidos en el presente estudio son muy similares a los del año 2010, de tal forma que una proporción importante de empresas señala que el límite máximo que podrían soportar en inactividad sería inferior a un día (afirmado por un 64,8% en 2012 y un 70,1% en 2010).

Según un estudio realizado por Deloitte en 2010[25], el 60,3% de las empresas consultadas señalaban que no podrían mantener sus actividades paralizadas durante más de 12 horas, mientras que un 27,3% indicaba que para que no existiera una incidencia importante se debían manejar márgenes de recuperación de menos de 2 días. Es importante destacar que el 87,7% de las empresas incluidas en este estudio tenían más de 100 trabajadores.

Gráfico 34: Evolución del tiempo máximo durante el que podría interrumpirse la actividad de la empresa sin suponer un impacto grave/crítico en el negocio (%)



Base 2012: total empresas (n=1.109) *Fuente: INTECO*
Base 2010: total empresa y casos de éxito (n=429)

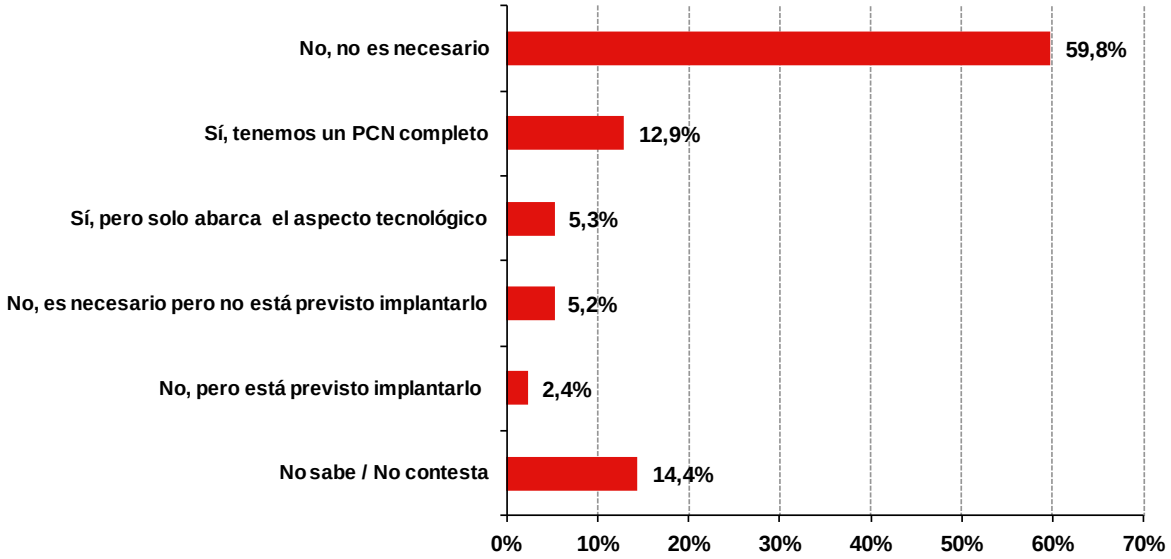
5.3.4 Desarrollo e implantación del Plan de Continuidad de Negocio

La disposición de Planes de Continuidad de Negocio implica asignar recursos humanos, económicos y técnicos a la labor de asegurar la continuidad de los procesos de negocio y, asimismo, permite tener una percepción más objetiva de los riesgos a los que se enfrenta, asegurando una respuesta organizada y consecuente.

[25]Ver Nota al pie 24.

A pesar de la criticidad de disponer de un Plan de Continuidad de Negocio, solo un 18,2% declara tenerlo implantado, bien con carácter integral (un 12,9%) bien enfocado a aspectos tecnológicos (5,3%). Por el contrario, casi seis de cada diez empresas no perciben que sea necesario.

Gráfico 35: Empresas que afirman disponer de un Plan de Continuidad de Negocio (%)



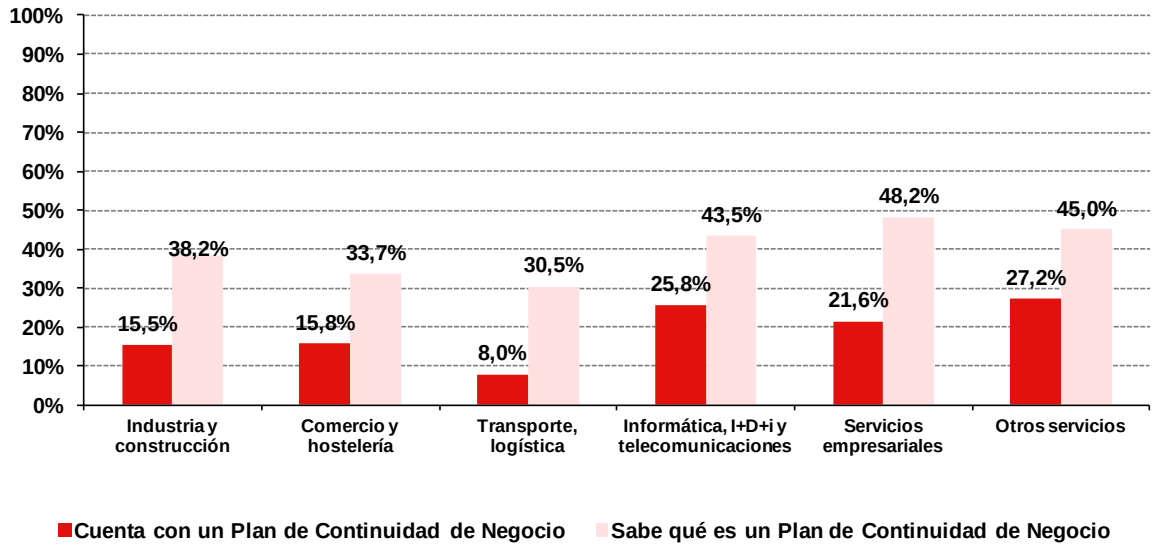
Base: Total empresas que responden a la parte de CN (n=1.109) *Fuente: INTECO*

En el siguiente gráfico se observa la existencia de una correlación positiva entre conocer y disponer de un Plan de Continuidad de negocio. En aquellas actividades donde el conocimiento es más amplio (como es el caso de los sectores de servicios y nuevas tecnologías), la implantación, aunque solo sea la parte tecnológica, es también más extensa.

En el extremo contrario, el sector de transporte aparece reflejado como el que conoce y dispone de un PCN en menor proporción. Sin embargo, el grado de detección de las actividades críticas era elevado. Esta diferencia en la percepción puede deberse a que, mientras que identifican que la continuidad de la actividad depende de los vehículos o de los permisos de circulación para poder ejercer la actividad (operaciones críticas), existe un desconocimiento del concepto Plan de Continuidad de Negocio aunque sí tienen previstas medidas alternativas para afrontar situaciones inesperadas.

Esta interpretación está en línea con lo indicado por los expertos en cuanto al desconocimiento terminológico como una explicación de la falta de concienciación de las pequeñas y medianas empresas ante los PCN. De la misma forma, los responsables de seguridad creen que *"se están utilizando medidas de continuidad, aunque en muchos casos no se identifiquen como tales".*

Gráfico 36: Conocimiento Vs. disposición en la empresa de un PCN, según sector de actividad (%)



Base: Total empresas que responden a la parte de CN (n=1.109) *Fuente: INTECO*

La gestión de la continuidad de negocio se aprecia en los diferentes aspectos contemplados dentro del Plan de Continuidad de Negocio. Como es lógico, existe una estrecha relación entre la estrategia de continuidad de las operaciones y el análisis de riesgos, como indica el 56% de las empresas. Asimismo, los PCN recogen aspectos como la asignación de responsabilidades (un 45,2% así lo señala), y la activación del plan de restablecimiento de las actividades de negocio principalmente (un 41,2%). La identificación de las operaciones críticas, actuación básica para la gestión de la continuidad, aparece por detrás, con un 36,6% que identifican esta medida dentro del PCN.

Por último, otras cuestiones como la evaluación del Plan y las acciones de comunicación son señaladas en menor proporción (32,2% y 31,9%, respectivamente).

Gráfico 37: Aspectos identificados dentro del PCN de la empresa (%)

Base: Empresas que disponen de un PCN (n=337) *Fuente: INTECO*

5.3.5 Evaluación de la eficacia del PCN

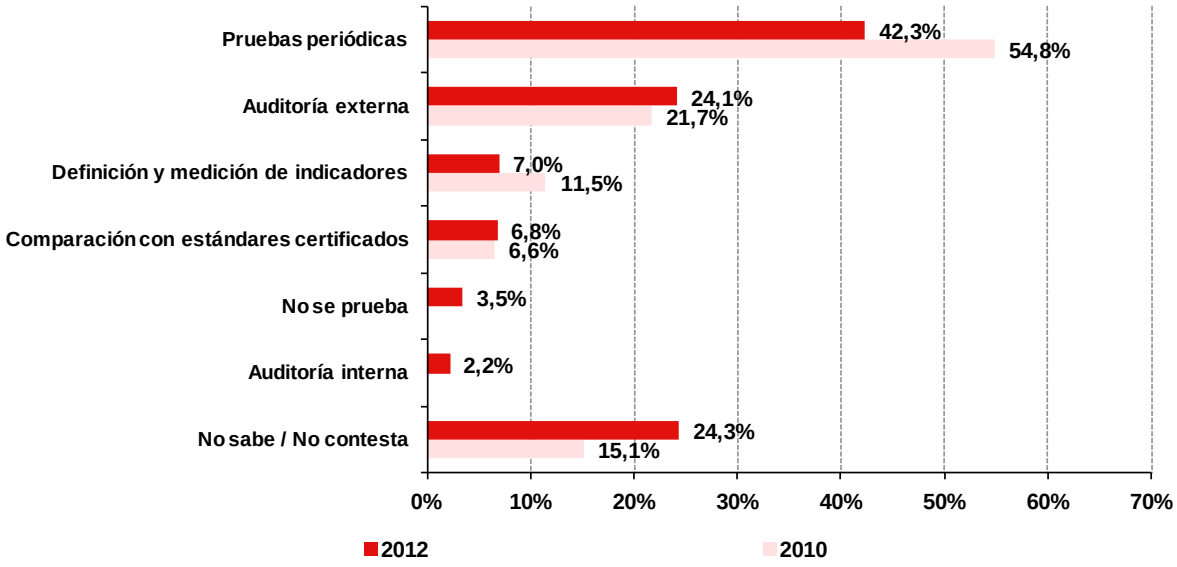
El Plan de Continuidad de Negocio está basado en la premisa de mejora continua, por lo que requiere establecer mecanismos para comprobar periódicamente su eficacia y rendimiento. En este sentido, según el estándar de continuidad de negocio BS 25999[26], es necesario probar periódicamente el Plan de Continuidad de Negocio para asegurar que las medidas están actualizadas y alineadas a las necesidades de disponibilidad de los procesos de negocio más críticos. Como se desprende del análisis anterior, del colectivo participante en el estudio, un 31,9% recoge la realización de pruebas como un componente del PCN.

Esta evaluación se lleva a cabo a través de diferentes actuaciones, siendo la más extendida la realización de pruebas periódicas, declarada por un 42,3%. Las empresas también recurren a auditorías externas (24,1%) como garantía de la efectividad de las medidas adoptadas.

Analizando la evolución con respecto a 2010, se observa que la disposición de mecanismos para probar la eficacia del PCN es similar. Las distintas opciones de medición son las mismas y tienen el mismo orden de importancia, aunque con distintos porcentajes.

[26] BS 25999: Se trata de una norma certificable en la que se tiene como objeto la Gestión o Plan de la Continuidad del Negocio fundamentalmente enfocado a la disponibilidad de la información. La 1ª parte, publicada en 2006, recoge un código de buenas prácticas en cuanto a CN. Esta primera parte es simplemente un documento de guía. La segunda parte establece los requisitos para un Sistema de Gestión de la Continuidad. Esta es la parte de la norma que se certifica a través de una etapa de implementación, de auditoría y posterior certificación.

Gráfico 38: Evolución de la disponibilidad de mecanismos para probar la eficacia del PCN en la empresa (%)



Base 2012: Empresas que disponen de un PCN (n=337) *Fuente: INTECO*
Base 2010: Empresas que disponen de una estrategia de CN (n=199)

5.3.6 Requerimientos a terceros en materia de continuidad de negocio

Por último, la actividad de las organizaciones requiere del suministro de determinados servicios por parte de proveedores externos, como por ejemplo la energía eléctrica, la conexión a Internet o la utilización de una infraestructura o plataforma de trabajo en la nube. La disposición de estos servicios influye directamente en la continuidad de negocio, por lo que este extremo debe formar parte de la estrategia de continuidad.

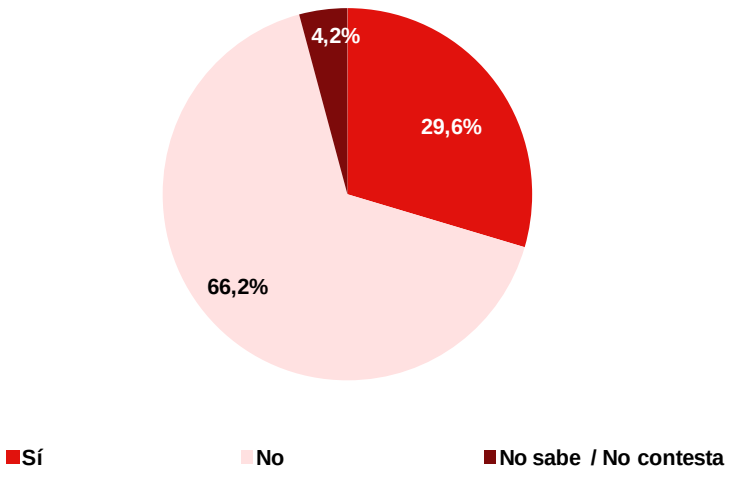
A la hora de negociar con el prestador de un servicio, se pueden alcanzar acuerdos de nivel de servicio[27] o planes de gestión de la continuidad. Sin embargo, el colectivo participante en el estudio no traslada esta preocupación por la continuidad de las operaciones a los terceros con los que trabaja: así, dos de cada tres empresas dicen no exigir a sus proveedores requisitos en materia de continuidad.

En línea con los análisis anteriores, existe una menor probabilidad de que las microempresas requieran de sus proveedores garantías de continuidad, mientras que las pequeñas y medianas empresas son más conscientes. Las organizaciones participantes en las entrevistas en profundidad señalan que "*los servicios de cobertura total frente a incidentes tienen un coste relativamente elevado y la rentabilidad no se aprecia en el corto plazo*", por lo que serán más

[27] Acuerdo de nivel de servicio o *Service Level Agreement* (ANS o SLA): son contratos que estipulan una serie de parámetros establecidos de mutuo acuerdo y que refleja el nivel operativo, el tipo de servicio, las garantías y respuestas, y las penalizaciones por caída de sistema, entre otras cuestiones.

probables en medianas y grandes empresas, generalmente con mayores necesidades de continuidad.

Gráfico 39: Empresas que afirman exigir a los proveedores algún nivel de servicio o un plan de gestión de la continuidad (%)



Base: Total empresas que responden a la parte de CN (n=1.109) *Fuente: INTECO*

6 INCIDENTES DE SEGURIDAD EN LA EMPRESA: INCIDENCIA, IMPACTO Y RESPUESTA

Una de las tendencias apuntadas por la industria de seguridad de la información para 2012 es el previsible aumento de los ataques dirigidos a la pequeña y mediana empresa[28]. La información –sobre clientes, proveedores, usuarios, etc. – que poseen las organizaciones es un activo de gran valor, que los atacantes tratan de obtener para traducir en lucro económico, prestigio como hackers o daño reputacional a la compañía afectada.

En el caso de la pequeña y mediana empresa, la limitación de sus recursos técnicos y humanos y el menor grado de implantación de buenas prácticas y políticas de seguridad respecto a las grandes empresas implica una mayor vulnerabilidad frente a estos incidentes y mayores consecuencias de los mismos en el caso de producirse, llegando incluso a afectar a la continuidad de las operaciones. La heterogeneidad de las empresas en cuanto a su grado de preparación frente a posibles riesgos se refleja asimismo en la forma de responder y combatir estos incidentes y sus impactos.

En el presente epígrafe se identifican los incidentes de seguridad de la información y continuidad de negocio que acontecen a las empresas, en qué medida les afectan y cuáles son las principales reacciones que adoptan.

Los resultados mostrados se basan en la percepción del colectivo entrevistado, por lo que pueden existir divergencias con la realidad. En cada gráfico, se menciona la base de cálculo empleada.

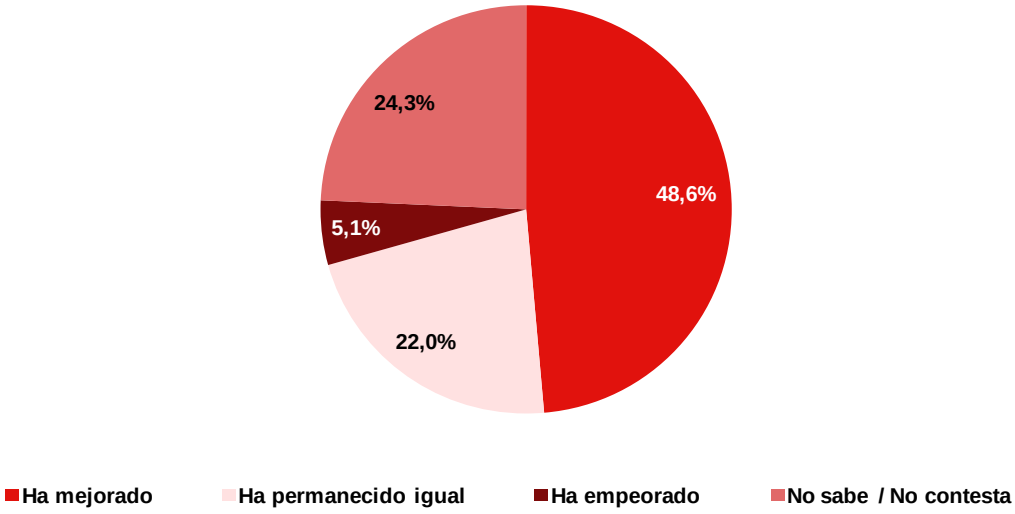
6.1 PERCEPCIÓN DE LAS EMPRESAS SOBRE LA EVOLUCIÓN GENERAL DE LOS INCIDENTES DE LA SEGURIDAD

En líneas generales, la percepción de las pequeñas y medianas empresas españolas en cuanto a la evolución de la seguridad en el último año es positiva: así lo opina cerca de la mitad de las empresas consultadas (un 48,6%). Un 22,0% señala que ha permanecido igual, mientras que para un 5,1% ha empeorado. Es destacable que cerca de una cuarta parte de los consultados no se manifiesta al respecto.

Por su parte, los expertos participantes en el estudio se muestran más escépticos con relación a la evolución de la seguridad de la información en el tejido empresarial español. Como indican los propios responsables de seguridad entrevistados, la relevancia pública de los casos de delitos informáticos resueltos por las fuerzas de seguridad provoca una falsa sensación de que los incidentes se resuelven y, por tanto, se percibe más seguridad.

[28] Fuente: PANDA SECURITY (2012). *Informe Anual Pandalabs 2011*.
http://prensa.pandasecurity.com/wp-content/uploads/2012/01/Informe-Anual-PandaLabs-2011.pdf

Gráfico 40: Evolución percibida en el último año sobre la seguridad en la empresa (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

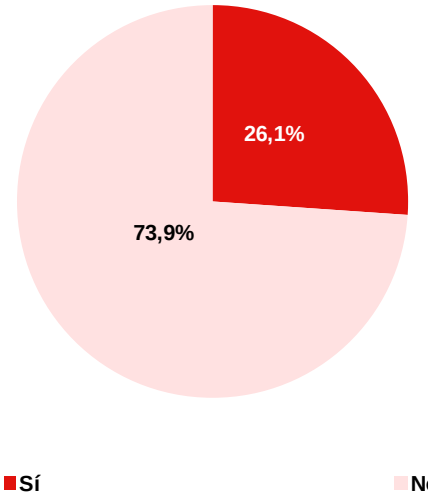
6.2 PERCEPCIÓN DE LAS EMPRESAS SOBRE SUS INCIDENTES DE SEGURIDAD

En el presente epígrafe se describe, con carácter general, la percepción de las empresa sobre los incidentes de seguridad sufridos en los sistemas TIC, incluyendo los que impactan en los dispositivos móviles y las tecnologías inalámbricas– cada vez más presentes en la operativa diaria de las compañías–, así como las situaciones de contingencia o crisis que pueden provocar la paralización de las actividades de la compañía.

6.2.1 Incidentes de seguridad de la información

Tres de cada cuatro empresas de menos de 250 empleados y con conexión a Internet afirman no tener constancia de haber sufrido incidentes de seguridad. No obstante, esta percepción no coincide plenamente con la realidad, ya que en opinión de los expertos consultados existe un amplio porcentaje de incidentes de seguridad que pasan desapercibidos.

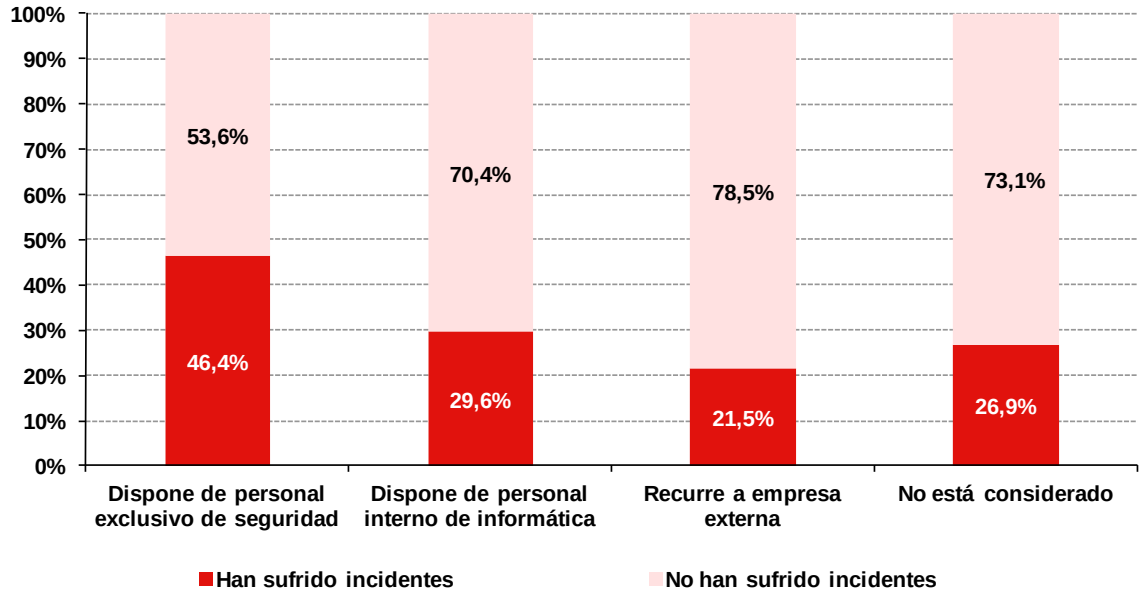
Gráfico 41: Empresas que afirman haber sufrido algún incidente de seguridad (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Corrobora esta idea el hecho de que existe una correlación entre las incidencias de seguridad y el disponer de recursos específicamente dedicados a la seguridad. Así, las empresas que disponen de personal dedicado en exclusiva son las que detectan mayor proporción de incidencias (46,4%), mientras que esta detección es menor si el personal no está especializado en seguridad (29,6%). Por su parte, las organizaciones que delegan la seguridad en terceros son las que menos casos perciben (21,5%).

Gráfico 42: Incidentes vs. disposición de personal dedicado a seguridad (%)

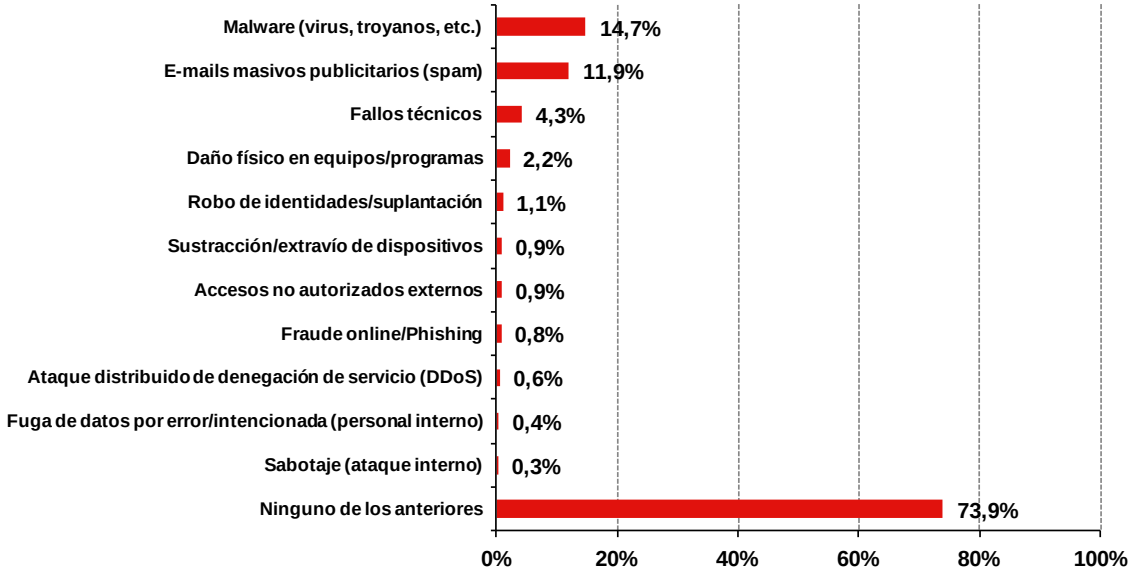


Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Entre las empresas que afirman haber sufrido algún tipo de incidente, los más frecuentes son la infección por malware (14,7%), la recepción de correo electrónico no deseado o spam (11,9%), los fallos técnicos (4,3%) y el daño físico en los equipos o programas (2,2%). En opinión de las empresas, el resto de incidencias se producen en menor proporción.

De las entrevistas en profundidad a los responsables de seguridad se extrae la percepción de que "no existe la seguridad total". Por su parte, los expertos en seguridad resaltan la baja declaración de incidentes como el robo de información, en parte porque las empresas prefieren que esa información no sea conocida públicamente.

Gráfico 43: Incidentes de seguridad reconocidos por las empresas (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Para completar este análisis, resulta interesante estudiar si los diferentes incidentes ocurren a las empresas de la misma manera o existen particularidades por tamaño.

En este sentido, las medianas empresas afirman sufrir incidentes en mayor proporción, mientras que las pequeñas y microempresas presentan una incidencia menor, con niveles similares en ambos colectivos. Una posible explicación puede estar en el hecho de que las empresas medianas son las que disponen de personal interno dedicado a la seguridad, lo que, como se reflejaba en el Gráfico 42, implica una mayor conciencia de los incidentes de seguridad sufridos.

A pesar de las diferencias, los incidentes más señalados (malware, spam, fallos técnicos y daños físicos) lo son para todos los tipos de empresa. La sustracción y extravío de dispositivos afecta casi exclusivamente a las medianas empresas (un 6,1% así lo declara, frente a un 0,9% en la micro y un 0,5% en la pequeña empresa).

Tabla 6: Principales incidentes de seguridad declarados por las empresas según tamaño (%)

	Microempresa	Pequeña empresa	Mediana empresa
Malware (virus, troyanos, etc.)	14,4	17,5	25,9
E-mails masivos publicitarios (spam)	11,9	11,9	21,6
Fallos técnicos	4,0	8,4	10,6
Daño físico en equipos/programas	2,1	2,8	10,4
Sustracción/extravío de dispositivos	0,9	0,5	6,1

Base: Microempresas (n=442), pequeña empresa (n=393), mediana empresa (n=309) *Fuente INTECO*

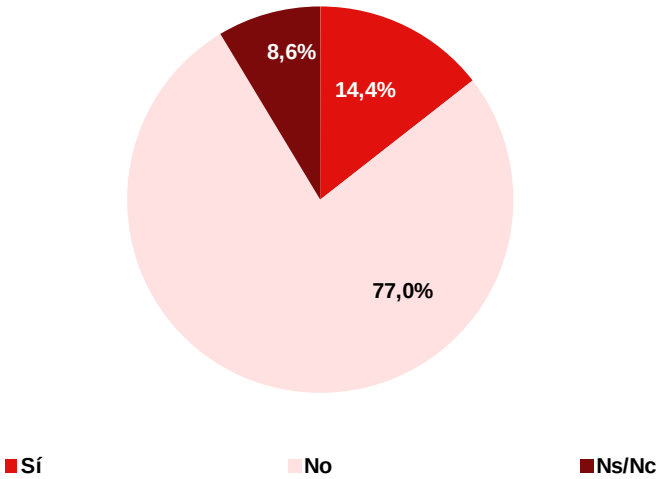
Los dispositivos móviles (como teléfonos móviles, smartphones, tabletas, etc.) se han convertido en pequeños equipos portátiles con multitud de funcionalidades que confieren a las empresas ventajas como la movilidad en las comunicaciones. Sin embargo, junto a los beneficios, también se heredan los posibles riesgos: malware, pérdida de información, etc.

En apartados anteriores, se observaba que los mecanismos de protección disponibles para los dispositivos móviles estaban integrados en menor medida que las herramientas de seguridad en los equipos informáticos, como afirmaban las empresas encuestadas.

A pesar de esto, el nivel de incidencia de situaciones de riesgo es ligeramente inferior al manifestado en cuanto al resto de equipamiento TIC.

De la investigación realizada se deduce que algo más de tres cuartas partes de las empresas (el 77,0%) señalan no haber tenido ningún percance de seguridad en sus terminales durante el último año, frente a un 14,4% que dice haber registrado alguno y un 8,6% que desconoce si ha ocurrido.

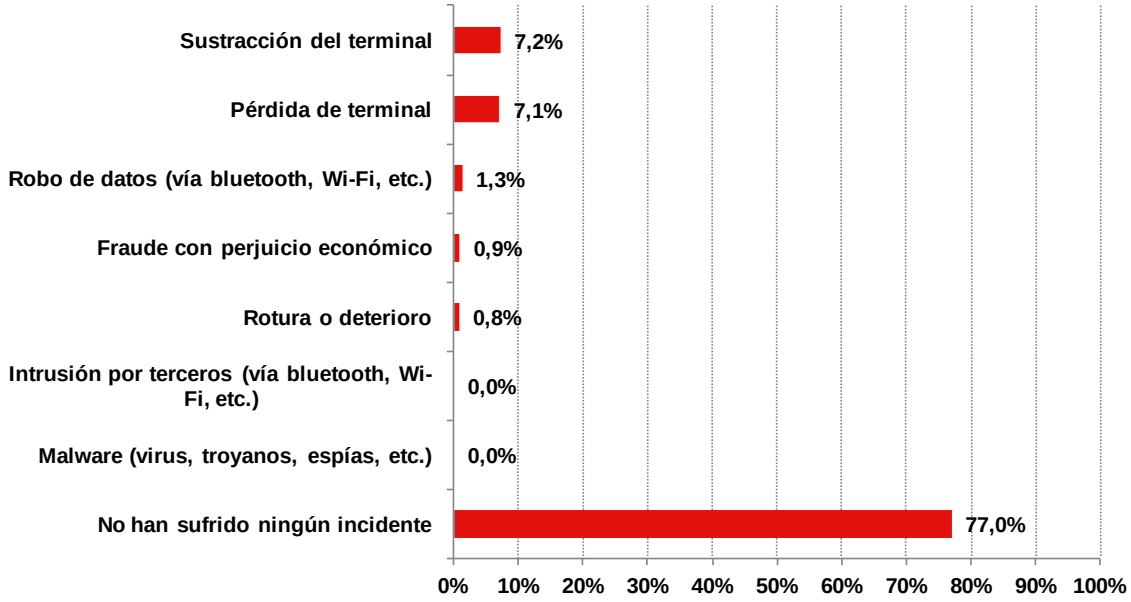
Gráfico 44: Incidentes de seguridad declarados en los dispositivos móviles (%)



Base: Empresas que cuentan con dispositivos móviles (n=459) *Fuente: INTECO*

Entre los incidentes ocurridos con mayor frecuencia, destacan la sustracción y la pérdida del terminal (7,2% y 7,1% respectivamente). Así mismo existen otras incidencias señaladas, aunque en menor medida, como el robo de datos (1,3%), fraude con perjuicio económico (0,9%), y rotura o deterioro (0,8%). Es reseñable que los incidentes relacionados con el malware en dispositivos móviles apenas son manifestados por el colectivo consultado.

Gráfico 45: Tipología de incidentes declarados en los dispositivos móviles (%)



Base: Empresas que cuentan con dispositivos móviles (n=459) *Fuente: INTECO*

El análisis por tamaño de la incidencia de situaciones que afectan a la seguridad de los dispositivos móviles permite extraer algunas conclusiones:

- Los incidentes más frecuentes (pérdida y sustracción de terminal) son declarados en mayor proporción por las medianas empresas.
- Las empresas pequeñas afirman en mayor medida que el resto haber sufrido fraude con perjuicio económico (7,6%), robo de datos (4,5%) y rotura o deterioro (1,2%).

Tabla 7: Incidentes declarados en los dispositivos móviles según tamaño (%)

Tipo de incidente	Microempresa	Pequeña empresa	Mediana empresa
Sustracción del terminal	7,2	6,2	9,4
Pérdida de terminal	6,7	10,0	21,9
Robo de datos (vía bluetooth, wifi, etc.)	1,1	4,5	0,7
Fraude con perjuicio económico	0,5	7,6	0,8
Rotura o deterioro	0,8	1,2	0,0
Intrusión por terceros (vía bluetooth, wifi, etc.)	0,0	0,1	0,7
Malware (virus, troyanos, espías, etc.)	0,0	0,1	1,1
No han sufrido ningún incidente	77,7	68,6	63,3

Base: Empresas con dispositivos móviles (micro n=135, pequeña n=153, mediana n=171)

En general, las medianas empresas disponen de un mayor número de dispositivos móviles, lo que aumenta las probabilidades de sufrir incidentes. Asimismo, cuentan en mayor medida de personal dedicado a la seguridad de la información y por tanto son las que tienen más capacidad para conocer los problemas más avanzados o técnicos como la intrusión o el malware en los móviles, mientras que en las pequeñas continúa siendo extraño.

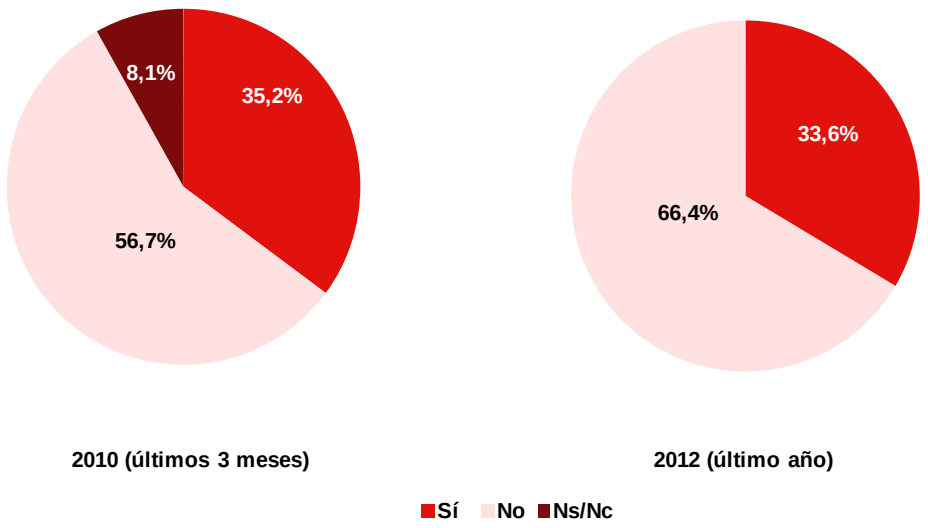
6.2.2 Incidentes que ponen en riesgo la continuidad del negocio

En ocasiones, las empresas deben afrontar determinados riesgos que, de materializarse, impactarían directamente sobre la disponibilidad de las actividades, provocando incluso la paralización del negocio.

En este apartado se examina la percepción de las pequeñas y medianas empresas sobre el impacto que determinados sucesos han tenido en la continuidad sus procesos u operaciones de negocio.

En primer lugar, una de cada tres empresas dice haber sufrido alguna circunstancia durante el último año que ha provocado la interrupción de las operaciones de negocio. Al observar la evolución de los valores en los dos últimos años, se observa un ligero descenso en la proporción de incidentes de este tipo declarados por las empresas, de un 35,2% en 2010 a un 33,6% en 2012. Es importante tener en cuenta que la pregunta formulada en 2010 se refería a los impactos registrados en los últimos tres meses, mientras que en la edición de 2012 el horizonte abarcado es el último año.

Gráfico 46: Incidentes de seguridad declarados que hayan impactado en la continuidad de los procesos u operaciones de negocio (%)



Base 2012: total empresas (n=1.109) *Fuente: INTECO*
Base 2010: total empresa y casos de éxito (n=429)

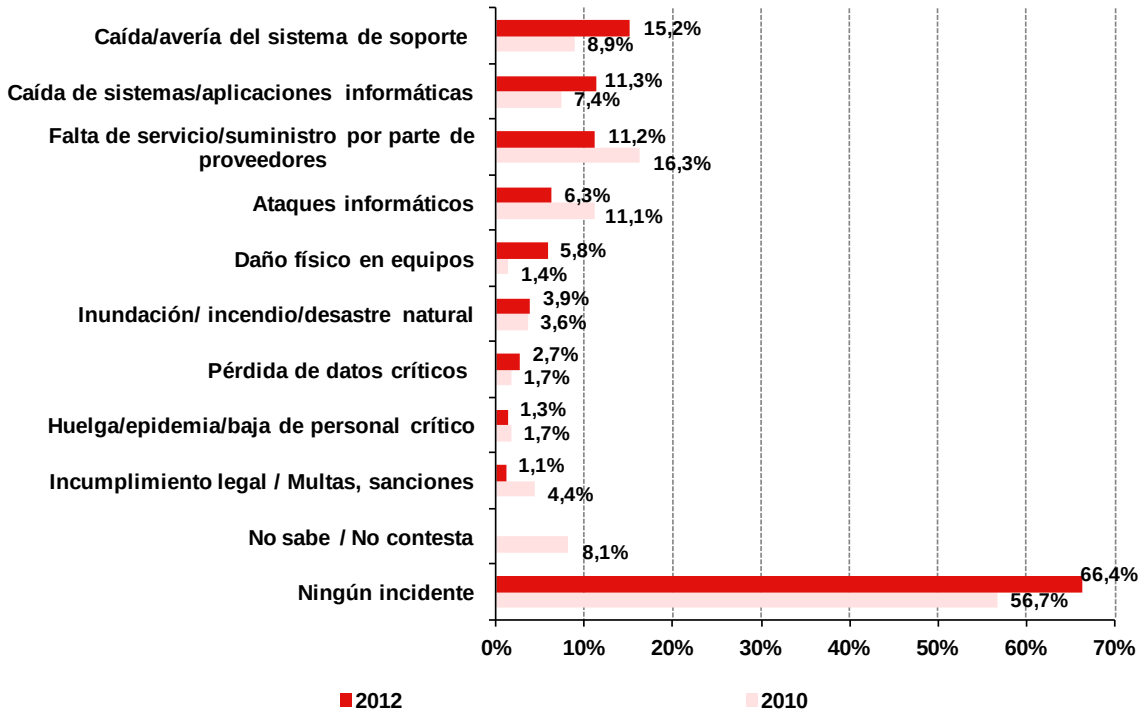
En segundo lugar, las empresas identifican incidentes de seguridad de índole muy variada que han puesto en peligro la continuidad de sus procesos.

En el último año, el principal incidente declarado es la caída o avería de los sistemas de soporte (un 15,2%), seguido de la caída de los sistemas o aplicaciones informáticas (11,3%) y la falta de servicio o suministro por parte de los proveedores (11,2%). En este caso, los ataques informáticos ocupan la cuarta posición como incidentes que pueden interrumpir el negocio, mientras que estaban en la primera posición en el ranking de incidentes de seguridad de la información (ver apartado 6.2.1 *Incidentes de seguridad de la información*).

Al comparar los valores con la incidencia declarada en 2010, destaca el aumento en la percepción de incidentes relacionados con el correcto funcionamiento de la infraestructura TIC interna (sistemas de soporte e informáticos), a la vez que descienden los achacables a los proveedores de suministros y los ataques de seguridad externos.

Se observa por tanto un cambio de relevancia, ya que en 2010 los proveedores eran la principal causa de incidentes, mientras que en la actualidad han sido relegados a un segundo plano.

Gráfico 47: Tipología de incidentes de seguridad que han impactado en la continuidad de los procesos u operaciones de negocio (%) [29]



Base 2012: total empresas (n=1.109) *Fuente: INTECO*
Base 2010: total empresa y casos de éxito (n=429)

6.3 IMPACTO Y CONSECUENCIAS DE LOS INCIDENTES

En el presente apartado se trata de responder a las siguientes cuestiones: ¿Qué efectos tienen los incidentes de seguridad vividos? ¿Con qué resultados? ¿Afectan a la continuidad de las operaciones de negocio?

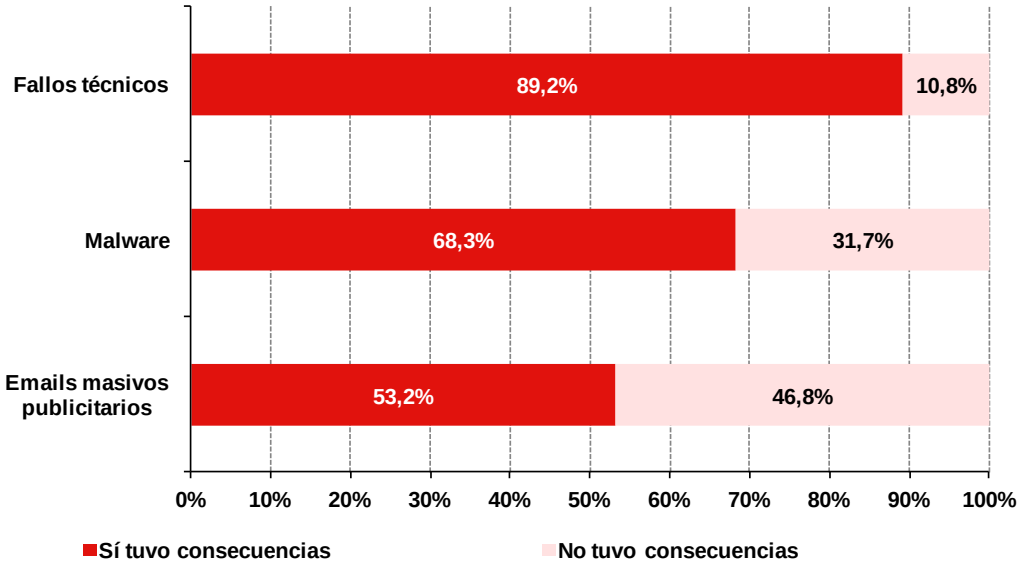
6.3.1 Consecuencias de los incidentes de seguridad de la información

En opinión del colectivo de pequeñas y medianas empresas que declaran haber sufrido algún incidente de seguridad, estos sucesos han tenido un impacto en su operativa, imagen o economía.

Teniendo en cuenta los tres incidentes más frecuentes, se analiza a continuación en qué proporción de sucesos se produjeron impactos para las organizaciones. Así, en un 89,2% de los casos de fallos técnicos, el percance tuvo consecuencias. También percibieron efectos negativos en un 68,3% de los casos de infección por y en un 53,2% del total de casos de spam.

[29] En 2010 se preguntó por "Multas o sanciones", mientras que en 2012 la categoría se formuló como "Incumplimiento legal".

Gráfico 48: Existencia de consecuencias derivadas de los principales incidentes de seguridad (%)



Fuente INTECO

La Tabla 8 muestra para cada uno de los tres principales incidentes de seguridad las diversas consecuencias que, en opinión de las empresas afectadas, experimentaron a raíz de dichos sucesos. En este caso, es necesario aclarar que las respuestas se ofrecen por empresas (no por sucesos) y que el grupo en cuestión podía identificar más de una respuesta en cada caso. Este análisis permite extraer una serie de conclusiones:

- En general, un porcentaje importante de las empresas percibe que las incidencias no han tenido consecuencias. Así lo señalan un 50,1% de las empresas que han recibido emails publicitarios de forma masiva y un 42,4% de los que han sufrido una infección por malware.

- Entre las que si señalan que se produjo algún efecto negativo, los señalados en mayor medida son los que afectan al tiempo y la productividad y los que implican una parada de las operaciones. Es decir, son consecuencias más visibles en un primer momento, mientras que las empresas son menos conscientes de haber sufrido impactos de naturaleza técnica.

- Sin embargo, la intensidad y el tipo de consecuencias varía para cada incidente. Para las empresas afectadas por fallos técnicos, estos incidentes han supuesto pérdidas de tiempo y productividad (66,9%), paradas (25,8%) y consecuencias técnicas (17,2%). En el caso de la infección por malware, los efectos más probables son pérdidas en la productividad (41,1%), seguidos de los costes relativos a la recuperación de los equipos (19,3%) y las consecuencias técnicas (10,5%). Por último, recibir spam ha supuesto una parada en la

actividad para un 37,7%, y en menor medida otros efectos derivados como el borrado de archivos (8,5%) o la pérdida de productividad (6,1%).

- Los incidentes más frecuentes para las organizaciones son, a su vez, los que han tenido en menor medida secuelas: las empresas perciben que el spam y el malware son las incidencias más usuales y, a su vez, señalan en mayor medida que estos no tuvieron consecuencias (15,5% y 42,4%, respectivamente).

Tabla 8: Consecuencias derivadas de los principales incidentes de seguridad (%)

Incidentes de seguridad	Fallos técnicos	Malware	Spam
Pérdida de tiempo/productividad	66,9	41,1	6,1
Parada en la actividad de mi empresa	25,8	5,3	37,7
Consecuencias técnicas	17,2	10,5	0,5
Costes de reparación/sustitución	7,6	19,3	3,5
Daños en la imagen /reputación	5,9	0,0	0,2
Borrado de archivos	0,6	6,3	8,5
Daños en hardware/software	0,5	4,6	0,4
Multas/sanciones por incumplimiento legal	0,5	-	-
Perjuicio económico (fraude)	0,5	-	-
Filtración de información confidencial/sensible	0,5	-	-
Cancelación de contratos clientes	0,5	-	-
No tuvo consecuencias	15,5	42,4	50,1
No sabe / No contesta	1,1	4,2	0,3

Base: empresas que han sufrido un incidente (malware n=199; emails masivos n=157; fallos técnicos n=90) *Fuente INTECO*

6.3.2 Consecuencias de los sucesos que afectan a la continuidad de negocio

Las situaciones de crisis, desastre o contingencia también generan impactos negativos para las empresas que los sufren. La Tabla 9 muestra las consecuencias que perciben las compañías para cada tipo de incidente sufrido en el último año. Se pueden extraer varias conclusiones del análisis:

- Los impactos operativos son los más destacados, independientemente del incidente vivido. Esta percepción coincide con la derivada de los incidentes en la seguridad de la información, relativa a la importancia que las empresas otorgan a las consecuencias cuyos efectos son más inmediatos.

- Los costes económicos son indicados principalmente por quienes han experimentado daños físicos en los equipos (46,3%), caídas en los sistemas informáticos o en la infraestructura de soporte (21,3% y 21,1%, respectivamente). Esta consecuencia se deriva del arreglo o sustitución de los mismos.

- Las empresas que han sufrido una caída de los sistemas o aplicaciones informáticos en el último año son las que identifican un mayor número de impactos derivados: junto a las consecuencias operacionales o económicas, estas empresas señalan también la pérdida

de clientes o impacto contractual (7,2%), el daño reputacional derivado del incidente (6,2%) o las sanciones a consecuencia del suceso (4,0 %).

- Los negocios que han sido víctimas de ataques informáticos señalan en mayor medida que el resto que estos incidentes no tuvieron consecuencias (el 36,7%), lo que denota un cierto desconocimiento del alcance de los mismos.

Tabla 9: Consecuencias que tuvo el incidente (%)

Consecuencias	Incidentes que afectan a la continuidad del negocio				
	Falta de servicio/ suministro por el proveedor	Caída de sistemas/ aplicaciones informát.	Fallo/ avería del sistema de soporte	Daño físico en equipos	Ataques informát.
Retrasos / horas perdidas / impacto en la productividad	83,9	81,8	73,4	70,2	52,7
Económico (coste directo)	14,6	21,3	21,1	46,3	10,4
Daño a la imagen de la empresa (impactos reputaciones)	2,0	6,2	4,4	4,9	2,1
Pérdida de clientes con los que existiera un contrato en firme (impacto contractual)	0,1	7,2	3,4	0,4	0,4
Sanciones / multas (impacto legal)	0,4	4,0	-	-	-
Otra consecuencia	0,3	0,1	0,1	-	4,3
Ningún impacto	9,8	7,5	10,6	10,0	36,7
No sabe/ No contesta	2,3	0,9	0,6	0,1	-

Base: Empresas que sufrieron incidentes de CN *Fuente INTECO*

6.4 RESPUESTA DE LAS EMPRESAS FRENTE A LOS INCIDENTES DE SEGURIDAD

Existen multitud de actuaciones que permiten reaccionar ante los incidentes que se producen en la empresa, aliviando en la medida de lo posible las consecuencias que estos provocan. En el presente apartado, se analiza cómo se han enfrentado las pequeñas y medianas empresas a las incidencias de seguridad sufridas en el último año.

Tras sufrir una situación de riesgo para la seguridad, un 38,5% de las empresas responden implementando cambios en sus hábitos, medidas o políticas de seguridad, frente a un 54,4% que no realiza ninguna modificación después de la experiencia y un 7,1% que no ofrece una respuesta.

Las empresas que adoptan una actitud activa ante un incidente responden actualizado o instalado herramientas de seguridad (19,7%) e implementando nuevas medidas como contraseñas y copias de seguridad (12,9%).

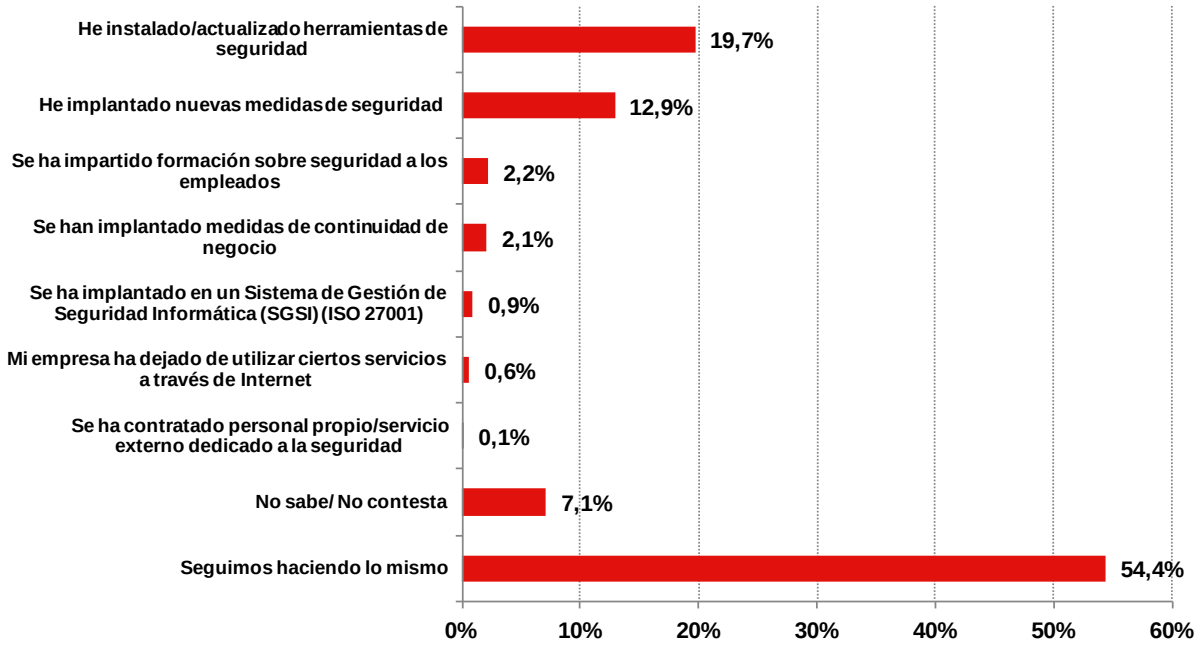
Por tanto, optan por medidas más inmediatas y menos costosas, frente a aquellas soluciones que implican el establecimiento de acciones formativas, estrategias internas de continuidad de negocio, certificaciones o refuerzo de personal de seguridad de la información.

A pesar de la tímida adopción de respuestas, destaca que las organizaciones no abandonan el uso de Internet tras sufrir un incidente, por lo que se puede afirmar que es una herramienta de trabajo imprescindible para las empresas.

Los expertos opinan respecto que "en muchas ocasiones las empresas no perciben haber sufrido incidentes, porque estas no han tenido un impacto grave en la empresa". Por otra parte señalan que las empresas que sí han tenido impactos no han cambiado la política de seguridad por "considerar que son hechos aislados". Esta falta de sensibilización ante las consecuencias derivadas de incidentes que afectan a la continuidad de negocio también es señalada por los responsables de seguridad de las empresas participantes en las entrevistas en profundidad.

Por último, el análisis en profundidad por sector de empresa indica que sectores como el de servicios empresariales (un 58,3%) y nuevas tecnologías (un 43,1%) son los más activos a la hora de realizar cambios tras sufrir un incidente.

Gráfico 49: Reacción adoptada tras los incidentes de seguridad (%)

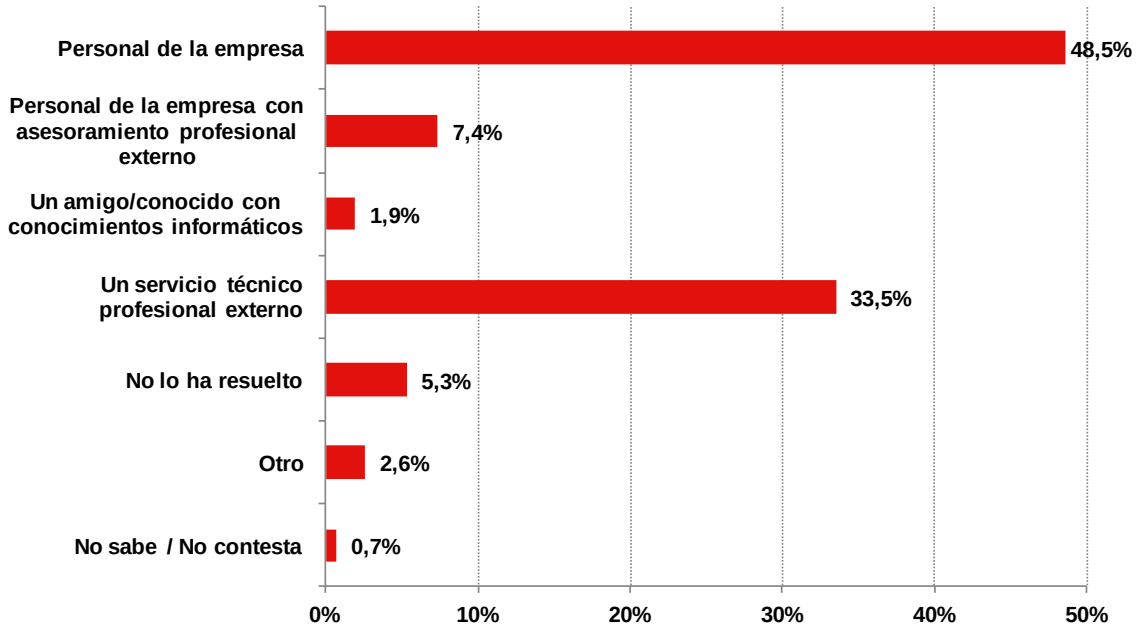


Base: Empresas que han sufrido algún incidente de seguridad (n=360) *Fuente INTECO*

En una organización, las incidencias pueden resolverse por varios medios: entre otras, por el propio personal de la empresa, con asesoramiento externo, con un servicio profesional externo, o a través de una persona de confianza con conocimientos informáticos.

Entre el colectivo entrevistado, el propio personal de la empresa es el encargado de dar respuesta al incidente (según declara un 48,5% de las empresas), si bien es notable la proporción de empresas que alegan que se apoyan en un servicio externo, bien para asesorar al personal de la empresa (un 7,4%), bien para resolver directamente el incidente (un 33,5%). No obstante, es significativo que un 5,3% de empresas no han llegado a resolver el incidente.

Gráfico 50: Resolución del incidente (%)



Base: empresas que han sufrido algún incidente de seguridad (n=360) *Fuente INTECO*

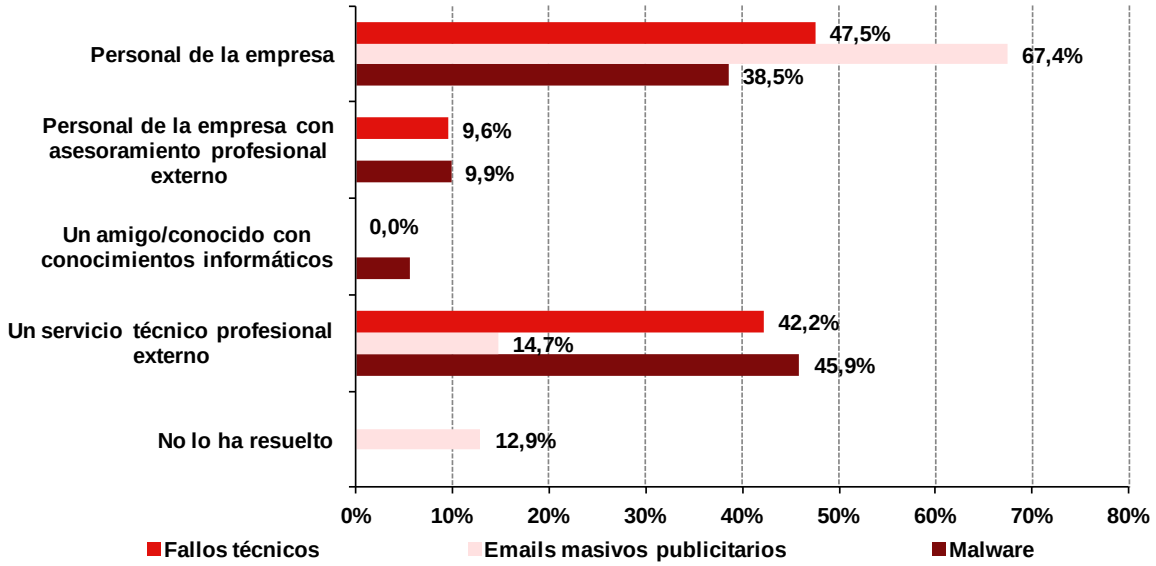
Por último, para conocer si el método de resolución está relacionado con el incidente sufrido, se profundiza en el análisis anterior atendiendo a los tres principales incidentes de seguridad: malware, spam y fallos técnicos.

- En este caso, los daños ocasionados de la infección por algún tipo de malware han sido reparados en mayor proporción a través de la subcontratación de un experto (un 45,9%), que por el personal interno (38,5%). Asimismo, un 9,9% declara que lo ha resuelto internamente, pero apoyándose en un consultor externo y un 5,6% han recurrido a amigos o conocidos para buscar una solución al incidente.

- En el caso de las incidencias relacionadas con los e-mails masivos publicitarios (spam), en gran parte de las ocasiones (un 67,4%) son los propios empleados los que tratan de dar respuesta. Frente a esta vía, sólo un 14,7% recurre a una intervención externa especializada, mientras que destaca la proporción de empresas que no lo resuelven (12,9%).

- Tras sufrir un fallo técnico, las empresas optan en proporciones similares por resolverlo internamente (47,5%) o contratando un servicio externo profesional, ya sea para resolverlo directamente (42,2%), o para proporcionarle asistencia (9,6%).

Gráfico 51: Resolución del incidente según el tipo de incidente vivido (%)



Base: empresas que han sufrido un incidente (malware n=199; emails masivos n=157; fallos técnicos n=90)

Fuente INTECO

7 E-CONFIANZA DE LA PEQUEÑA Y MEDIANA EMPRESA ESPAÑOLA

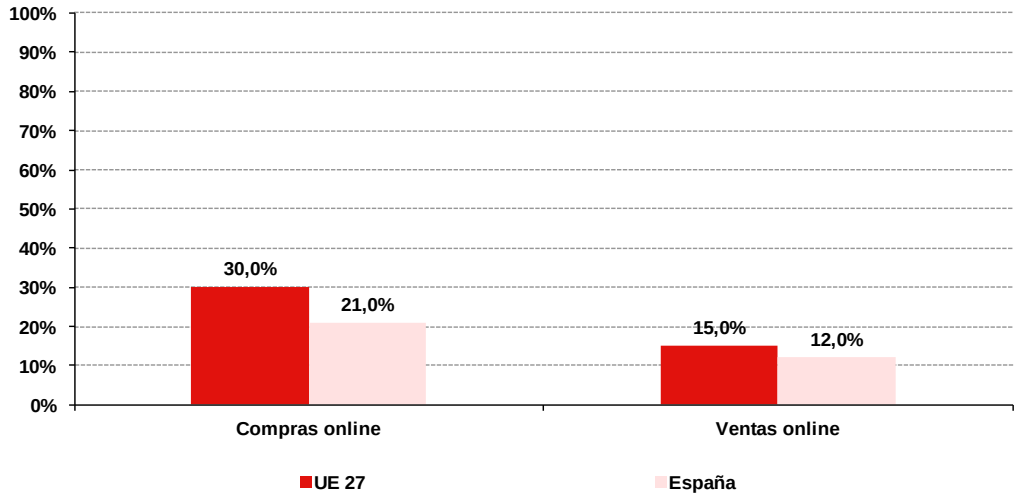
En la actualidad, Internet es para la gran mayoría de las empresas una herramienta de trabajo fundamental a través del cual realizan múltiples gestiones. Su uso está muy extendido, aunque no todas las organizaciones utilizan todas las posibilidades y servicios que ofrece.

En este sentido, el estudio de la e-confianza permite conocer la aceptación, familiaridad y seguridad con que las empresas abordan la adopción de servicios de la Sociedad de la Información. Para ello, se analizan las siguientes cuestiones:

- Nivel de utilización de servicios de la Sociedad de la Información.
- En base a las empresas que utilizan cada uno de los servicios, la confianza generada por dicho servicio.
- En base a las empresas que no utilizan cada uno de los servicios, los motivos alegados para no hacerlo.

Como primera aproximación, el siguiente gráfico muestra datos de Eurostat referidos a 2010[30] en cuanto a comercio electrónico en la empresa, comparando la penetración en España frente a la de la Unión Europea (27 países). Así, se parte de un comportamiento similar de España con respecto al conjunto de Europa, si bien las cifras de utilización nacionales se sitúan en todos los casos por debajo de las europeas. Esto indica un panorama inicial en el que existe la necesidad de impulsar la adopción de servicios en línea por parte de las empresas.

Gráfico 52: Utilización de servicios de Internet en la empresa. Comparativa europea (%)



Base= Total empresas con ordenador *Fuente: EUROSTAT (2010)*

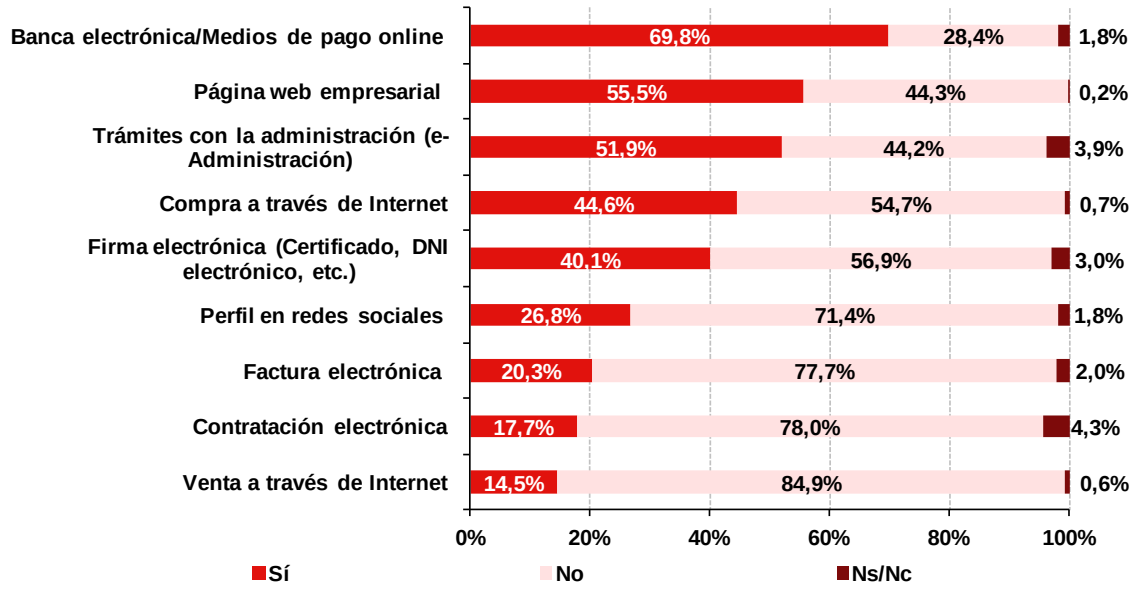
[30] Fuente: eMarket Services Spain ICEX (2011) *El comercio electrónico en España – 2011*. Disponible en: http://www.emarketservices.es/icex/cma/contentTypes/common/records/mostrarDocumento/?doc=4528333

Entre el colectivo participante en el estudio, la banca electrónica y medios de pago online son los servicios más extendidos, según afirma un 69,8%, mientras que recursos como la página web empresarial o la realización de trámites con la Administración Pública también son utilizados de forma considerable (un 55,5% y un 51,9%, respectivamente).

Menos de la mitad de las empresas participantes señala utilizar servicios como la compra a través de Internet (44,6%) y la firma electrónica (40,1%).

Por último, los servicios con menor presencia entre las pequeñas y medianas empresas son los perfiles en redes sociales (26,8%%), la factura electrónica (20,3%), la contratación electrónica (17,7%) y la venta online (14,5%).

Gráfico 53: Utilización declarada de servicios electrónicos a través de Internet por parte de las empresas (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Como viene ocurriendo, el tamaño de la empresa influye directamente en el grado de utilización de los servicios. Asimismo, se mantienen las posiciones en la parte alta de la tabla: banca electrónica, página web y e-Administración son los servicios más utilizados en todos los casos. Destaca el caso del comercio a través de Internet, declarado en mayor proporción por las microempresas.

Estos valores están en línea con los últimos datos publicados por ONTSI en cuanto al uso de las TIC por parte de las empresas españolas[31], si bien los datos son más coincidentes en el caso de pequeñas y medianas empresas y presentan mayores desviaciones en el caso de microempresas.

[31] Fuente: ONTSI (2012) Informe Anual "La Sociedad en Red", Edición 2011. Disponible en: http://www.ontsi.red.es/ontsi/es/estudios-informes/informe-anual-2011-edicion-2012

Tabla 10: Utilización de servicios electrónicos a través de Internet por parte de las empresas, según tamaño (%)

Servicios	Microempresa	Pequeña empresa	Mediana empresa
Banca electrónica/medios de pago online	69,1	79,9	81,4
Página web empresarial	54	77	91,4
Trámites con la administración (e-Administración)	50,8	69,1	88
Compra a través de Internet	45	36,9	42,8
Firma electrónica (Certificado, DNI electrónico, etc.)	38,7	59,3	77,1
Perfil en redes sociales	26,9	25,3	32,5
Factura electrónica	20	24,5	36,9
Contratación electrónica	17,3	23,4	32,4
Venta a través de Internet	14,2	17,6	21,4

Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

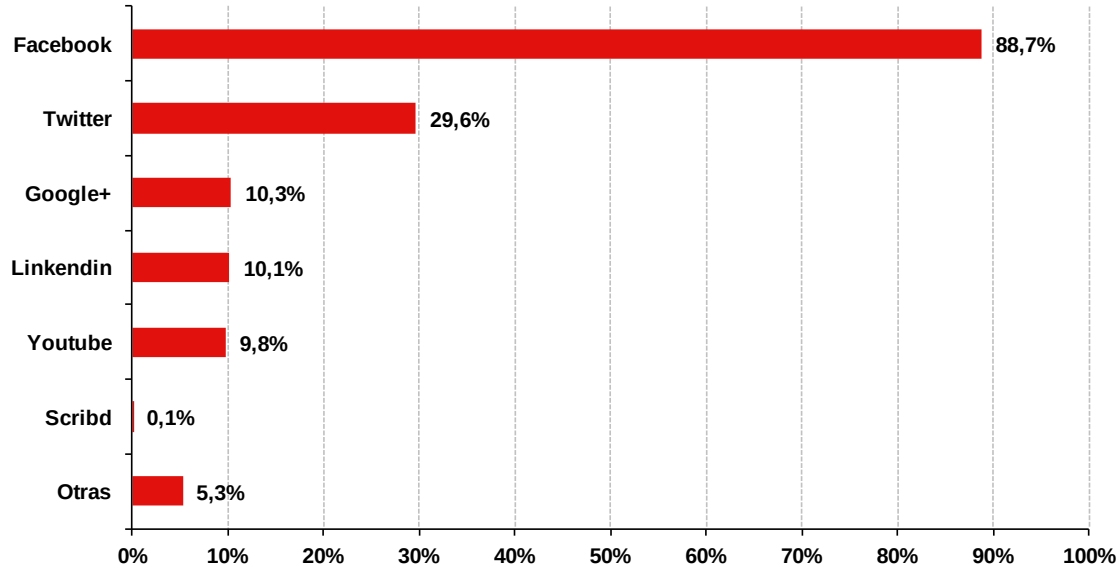
De todos los servicios analizados, las redes sociales han ganado protagonismo como canales de comunicación en las empresas, y se prevé que esta presencia siga aumentando en el futuro[32], por lo que resulta interesante estudiar la e-confianza que las empresas depositan en las redes sociales.

De las empresas que manifiestan disponer de perfiles o páginas en redes sociales, un 88,7% se encuentra en Facebook. A gran distancia se colocan redes sociales como Twitter (29,6%), Google+ (10,3%), LinkedIn (10,1%) o Youtube (9,8%).

La madurez en el mercado (con más de 700 millones de usuarios) y versatilidad de Facebook, que proporciona perfiles específicamente diseñados para empresas, puede explicar la preferencia mostrada por las compañías entrevistadas, frente a redes más orientadas a fines empresariales o profesionales, como Twitter o LinkedIn.

[32] Un 82% de pequeñas y medianas empresas declara que su presencia en redes sociales crecerá en el futuro. Fuente: Fundación Banesto en colaboración con el Ministerio de Industria Turismo y Comercio y la Empresa Nacional de Innovación (ENISA) (2011) *Observatorio sobre el uso de las redes sociales en las PYMEs españolas*. Estudio realizado para una muestra de n=2250 empresas de hasta 50 empleados. Disponible en: http://www.inteco.es/studyCategory/Seguridad/Observatorio/Biblioteca/observatorio_redes_sociales_FB

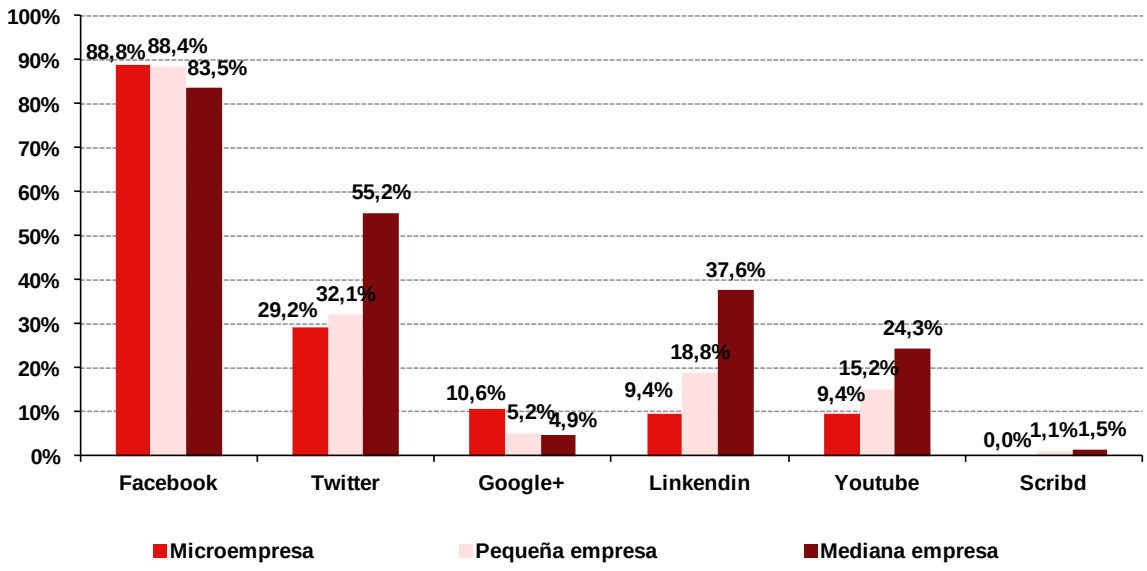
Gráfico 54: Presencia de las empresas en las diferentes redes sociales (%)



Base: Empresas que disponen de perfil en redes sociales (n=344) *Fuente: INTECO*

El análisis realizado por tamaño indica que las empresas con mayor número de empleados tienen más presencia en redes como Twitter, LinkedIn y Youtube, lo que puede indicar que las empresas medianas diversifican más su presencia en redes sociales.

Gráfico 55: Presencia de las empresas en las diferentes redes sociales, según tamaño (%)



Base: Empresas que disponen de perfil en redes sociales (n=344) *Fuente: INTECO*

7.1 E-CONFIANZA EN LA SOCIEDAD DE LA INFORMACIÓN

En el presente apartado se estudia el nivel de confianza que las empresas dicen otorgar a los diferentes servicios de Internet que utilizan. El análisis se divide en cinco bloques:

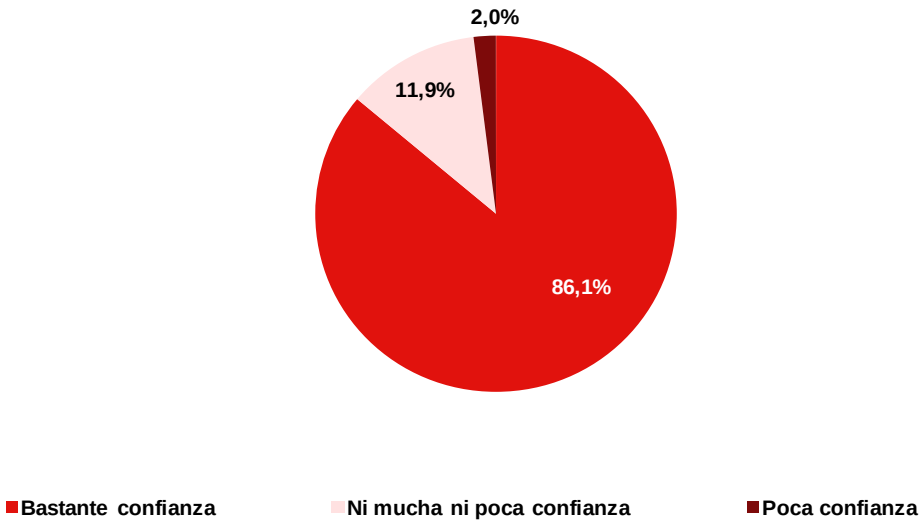
- Banca electrónica y medios de pago online.
- Compra y venta a través de Internet.
- Página web empresarial y redes sociales.
- Trámites con la Administración.
- Negocio electrónico: firma electrónica, factura electrónica y contratación electrónica.

7.1.1 E-confianza en la banca a través de Internet

Las empresas utilizan Internet como herramienta imprescindible para la gestión empresarial, puesto que permite realizar operaciones en línea de forma ágil y sencilla. Los servicios de banca electrónica y medios de pago online, los más extendidos entre las empresas (un 69,8% así lo señalaba), obtienen una alta valoración en cuanto al grado de confianza que les otorgan las empresas usuarias (un 86,1%).

El análisis por tamaño presenta valores similares en todos los casos.

Gráfico 56: Grado de confianza de las empresas en la utilización de la banca electrónica y los medios de pago online (%)



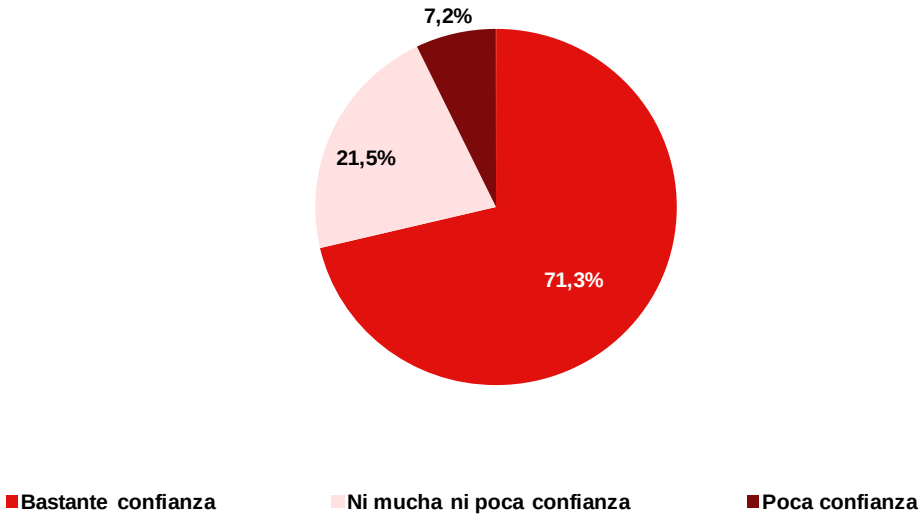
Base: Empresas que utilizan la banca electrónica y los medios de pago online (n=884) *Fuente: INTECO*

7.1.2 E-confianza en la compra y venta a través de Internet

Además de la realización de trámites bancarios en línea, las empresas utilizan Internet para facilitar las operaciones de compra a proveedores y venta a clientes.

Un 44,6% ha señalado realizar compras a través de Internet. Las organizaciones participantes dicen confiar mucho en este servicio, puesto que un 71,3% otorgan bastante confianza.

Gráfico 57: Grado de confianza de las empresas en las compras a través de Internet (%)



Base: Empresas que utilizan las compras a través de Internet (n=512) *Fuente: INTECO*

A medida que crece el número medio de empleados, aumenta la confianza mostrada. Mientras el 84,5% de la mediana empresa otorga bastante confianza a este servicio, en el caso de las microempresas este porcentaje desciende en 13,4 puntos porcentuales situándose en el 71,1%.

Tabla 11: Grado de confianza en la compra a través de Internet, según tamaño (%)

Grado de confianza	Microempresa	Pequeña empresa	Mediana empresa
Bastante confianza	71,1	75,1	84,5
Ni mucha ni poca confianza	21,6	19,8	14,1
Poca confianza	7,3	5,1	1,4

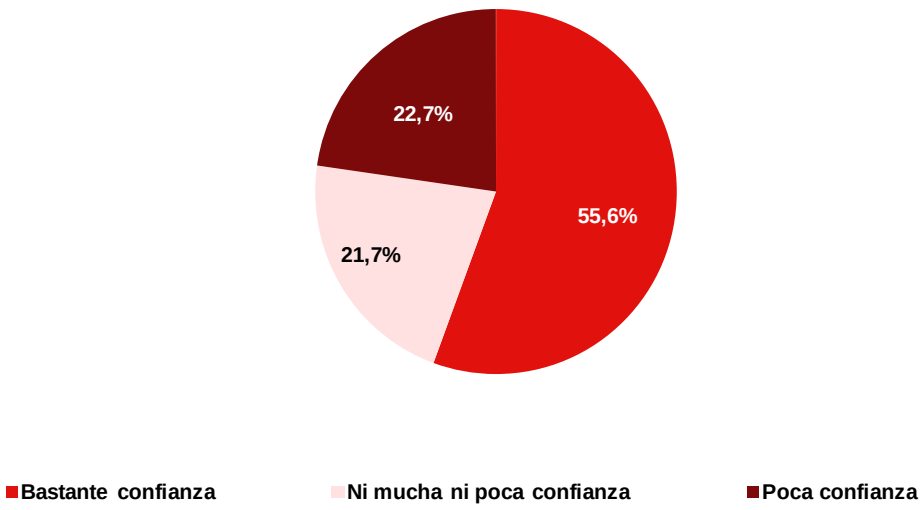
Base: Empresas que utilizan las compras a través de Internet (n=512) *Fuente: INTECO*

Otro de los servicios de Internet utilizado dentro de la gestión empresarial es el relativo a las ventas online a clientes (declarado por un 14,6% de las empresas).

En este caso, más de la mitad de las empresas (un 55,6%) declara que este servicio les genera bastante confianza. Es destacable la diferencia en la valoración que las empresas conceden a este servicio con respecto a la compra a través de Internet (71,3%).

Esta menor confianza es corroborada por los responsables de seguridad consultados en las entrevistas en profundidad, quienes "ven necesario mejorar la seguridad de los pagos, por ejemplo a través del fomento de certificados". Con campañas de publicidad que expliquen claramente el fenómeno del fraude ligado al comercio electrónico y las medidas para evitarlo y/o combatirlo, se mejoraría (a juicio de estos profesionales) la penetración de los servicios de compra y venta online.

Gráfico 58: Grado de confianza de las empresas en la venta a través de Internet (%)



Base: Empresas que utilizan la venta a través de Internet (n=200) *Fuente: INTECO*

El análisis por tamaño muestra una vez más la relación positiva entre el tamaño y la valoración, de forma más marcada. Así el 83,2% de las medianas empresas muestra bastante confianza, porcentaje que desciende al 54,1% en el caso de las empresas de menor tamaño. Estas últimas, a su vez, son las que indican tener poca confianza (23,8%) en mayor proporción que el resto.

Tabla 12: Grado de confianza en la venta a través de Internet, según tamaño (%)

Grado de confianza	Microempresa	Pequeña empresa	Mediana empresa
Bastante confianza	54,1	74,8	83,2
Ni mucha ni poca confianza	22,1	16,0	15,7
Poca confianza	23,8	9,2	1,1

Base: Empresas que utilizan la venta a través de Internet (n=200) *Fuente: INTECO*

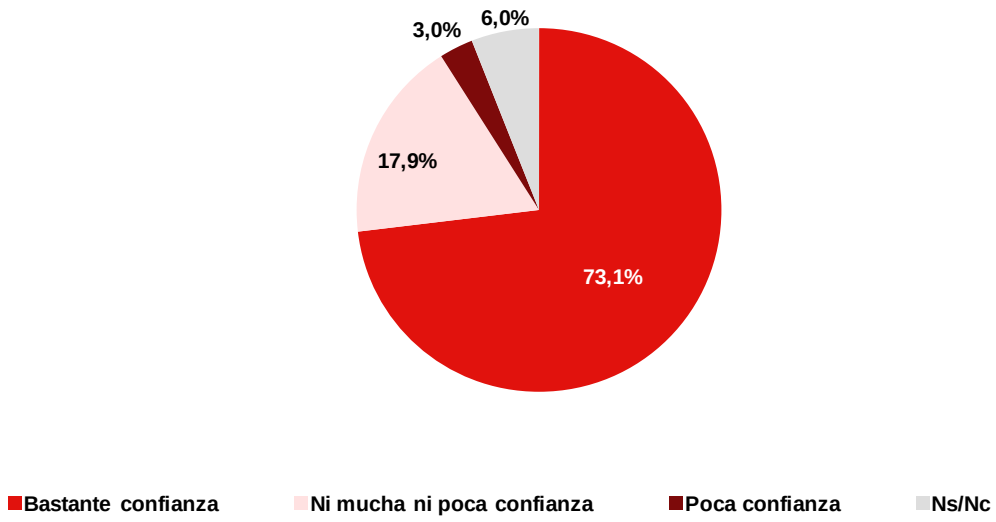
7.1.3 E-confianza en la utilización de página web empresarial y redes sociales

La disposición de una **página web empresarial** ofrece a las empresas múltiples beneficios, ya que propicia la presencia de la empresa en Internet, facilita el contacto con sus proveedores, clientes o usuarios, y permite mostrar y/o vender a un mayor número de potenciales clientes sus productos o servicios.

Aquellas compañías que disponen de página web de empresa (55,5%) muestran un elevado nivel de confianza en este servicio (un 73,1% afirman que les genera mucha confianza).

No se aprecian diferencias significativas en función del tamaño de empresa.

Gráfico 59: Grado de confianza de las empresas en la utilización de página web corporativa (%)



Base: Empresas que utilizan la página web corporativa (n=849) *Fuente: INTECO*

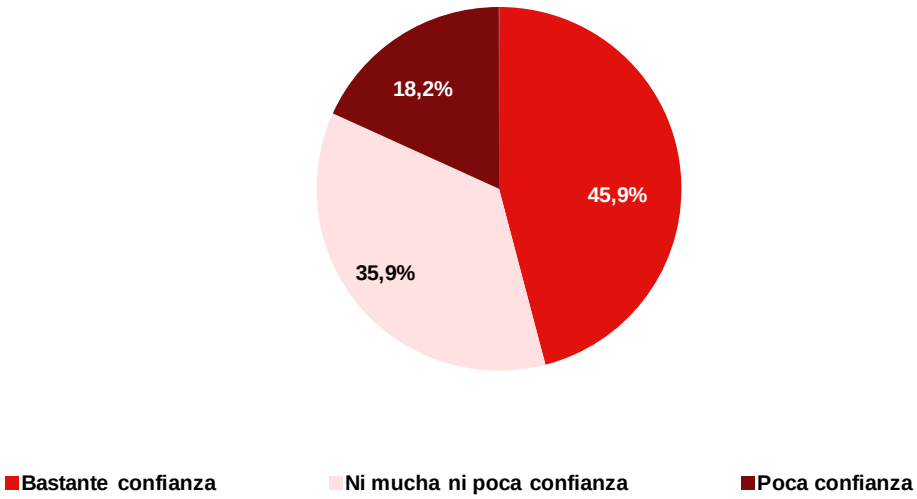
Las **redes sociales** son un canal de comunicación abierto y dinámico que complementa a la página oficial de la empresa a la hora difundir la imagen de marca y los servicios que ofrece, facilitando la interacción con los proveedores, clientes y usuarios, ya sean reales o potenciales. Estos servicios son relativamente novedosos, por lo que todavía muchas empresas no disponen de perfiles activos en redes de este tipo.

Así, en el momento de realización del estudio, un 26,8% de las empresas dicen tener una presencia activa en redes sociales. Según los responsables de las empresas participantes en las entrevistas en profundidad, “las redes sociales aportan ventajas como la mayor excelencia en el servicio, al proporcionar un canal de comunicación directo para el trato con el cliente”. También se señalan desventajas, como “la inversión en tiempo que se requiere para atender estos canales”.

En este caso, la confianza mostrada respecto a este tipo de redes es menor que la mostrada sobre la página web empresarial: un 45,9% de las empresas otorga bastante confianza a las redes

sociales, frente a un 73,1% en el caso de la página web. Cabe destacar que el 35,9% se muestran indiferentes y un 18,2% afirma que las redes sociales les generan poca confianza.

Gráfico 60: Grado de confianza de las empresas en la utilización de redes sociales (%)

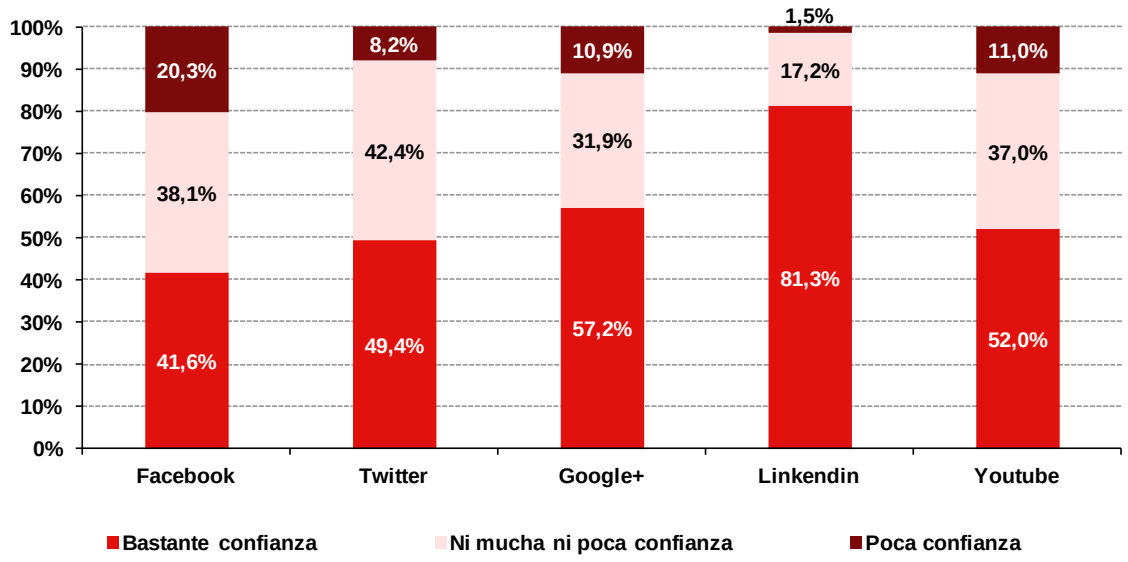


Base: Empresas que utilizan las redes sociales (n=344) *Fuente: INTECO*

A pesar de que Facebook es la red social más extendida, no es la que genera mayores niveles de confianza. Para un 81,3% de las empresas que utilizan LinkedIn, este canal les genera bastante confianza, seguido de Youtube (52,0%) y Twitter (49,4%). En el lado opuesto un 20,3% de las usuarias de Facebook se muestran desconfiadas.

Los expertos consideran que, a pesar de que Facebook es la red social más extendida, Linkedin es la que tiene una utilidad más clara para las organizaciones, al tener una orientación más profesional. Esta idea también es refrendada por los responsables de seguridad de las empresas participantes en las entrevistas en profundidad, quienes confían más en LínkedIn y señalan a Facebook como “un fenómeno influido por las modas”.

Gráfico 61: Grado de confianza de las empresas en la utilización de redes sociales, en función de la red social utilizada (%)



Base: Empresas que utilizan las redes sociales (n=344) *Fuente: INTECO*

7.1.4 E-confianza en los trámites con la Administración

En su día a día, las organizaciones realizan numerosos trámites con la Seguridad Social, la Agencia Tributaria, etc. Los **servicios de Administración electrónica** permiten agilizar las gestiones, al no existir la necesidad de trasladarse físicamente al espacio donde se llevan a cabo los trámites, sino que existe un espacio virtual para llevarlos a cabo.

En términos globales, algo más de la mitad de las empresas consultadas (el 51,9%) afirman realizar estos trámites en línea. La valoración que otorgan a la e-Administración es muy positiva, ya que casi nueve de cada diez muestran bastante confianza.

No se aprecian diferencias significativas en función del tamaño, sino que se puede afirmar que las empresas españolas confían en la realización de operaciones con la Administración a través de la Red.

Gráfico 62: Grado de confianza de las empresas en los trámites con la Administración (%)

Base: Empresas que utilizan los trámites con la Administración (n=781) *Fuente: INTECO*

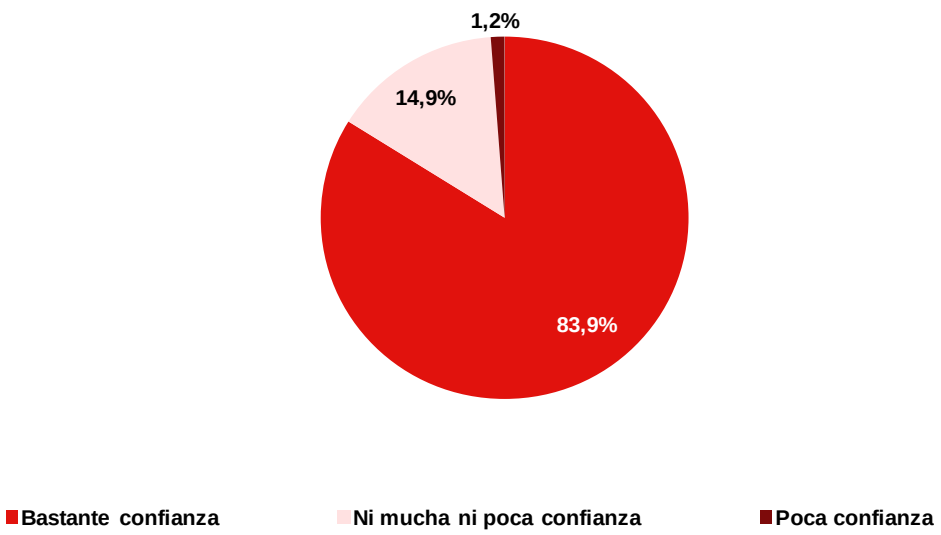
7.1.5 E-confianza en el negocio electrónico

La **firma electrónica** es un mecanismo que permite a su titular asegurar la identidad del firmante y la integridad del mensaje. Con la firma electrónica se pueden acreditar la identidad del autor y, en caso de documentos compartidos, fijar el contenido del documento mediante el cruce de copias firmadas por todas las partes implicadas.

El empleo de la firma electrónica requiere el uso de la tecnología para asignar a los datos identificativos del titular del certificado una serie de claves vinculadas a él.

La utilización de este mecanismo genera una elevada confianza (un 83,9%) entre las empresas que afirman disponer de este mecanismo. De las entrevistas en profundidad realizadas a los responsables de seguridad de las empresas, se extrae una valoración positiva de este mecanismo, pero también demandas como “fomentar la concienciación y formación en el uso”, así como “facilitar y armonizar los procedimientos de obtención de la firma electrónica”.

Gráfico 63: Grado de confianza de las empresas en la firma electrónica (%)



Base: Empresas que utilizan la firma electrónica (n=669) *Fuente: INTECO*

La firma electrónica sugiere un mayor nivel de confianza entre las empresas pequeñas y medianas (ambas por encima del 90%), siendo algo inferior en el caso de las microempresas (83,3%).

Tabla 13: Grado de confianza en la firma electrónica, según tamaño (%)

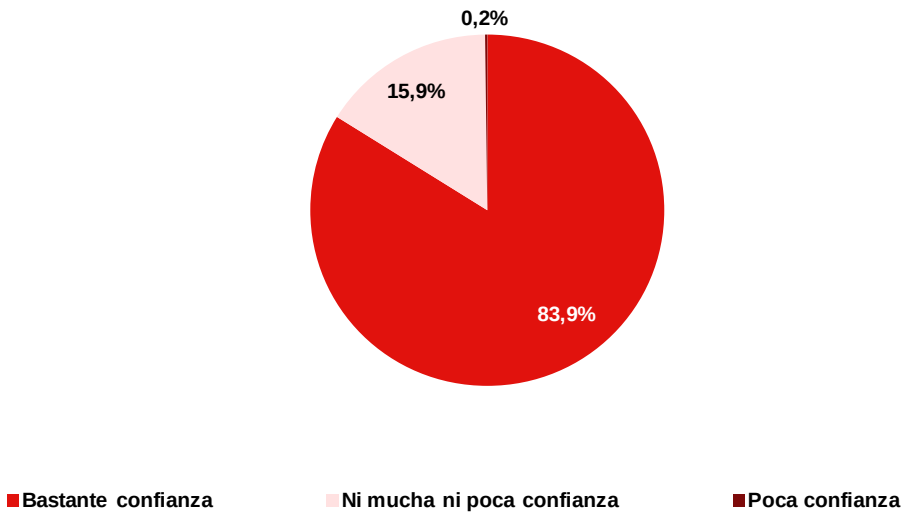
Grado de confianza	Microempresa	Pequeña empresa	Mediana empresa
Bastante confianza	83,3	91,4	91,6
Ni mucha ni poca confianza	15,5	8,3	8,4
Poca confianza	1,2	0,3	0,0

Base: Empresas que utilizan la firma electrónica (n=669) *Fuente: INTECO*

Por su parte, la **factura electrónica** es un documento electrónico transmitido de forma telemática y que una vez emitido garantiza la identidad del emisor y la integridad de todo su contenido, dado que se encuentra firmado mediante certificado de firma electrónica reconocida. La factura electrónica cumple con los requisitos legal y reglamentariamente exigibles a las facturas y, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor. La finalidad última de la factura electrónica es poder prescindir de las facturas en formato papel, manteniendo la validez legal plena del documento.

A pesar de que este servicio no está muy extendido (el 20,3%), el grado de confianza depositado entre los usuarios es elevado, puesto que el 83,9% así lo señala.

Gráfico 64: Grado de confianza de las empresas en la factura electrónica (%)



Base: Empresas que utilizan la factura electrónica (n=317) *Fuente: INTECO*

Las empresas de mayor tamaño muestran mayor confianza en el uso de la factura electrónica que las microempresas. Prácticamente la totalidad de empresas medianas confieren bastante confianza en este servicio (el 93,6%).

Tabla 14: Grado de confianza en la factura electrónica, según tamaño (%)

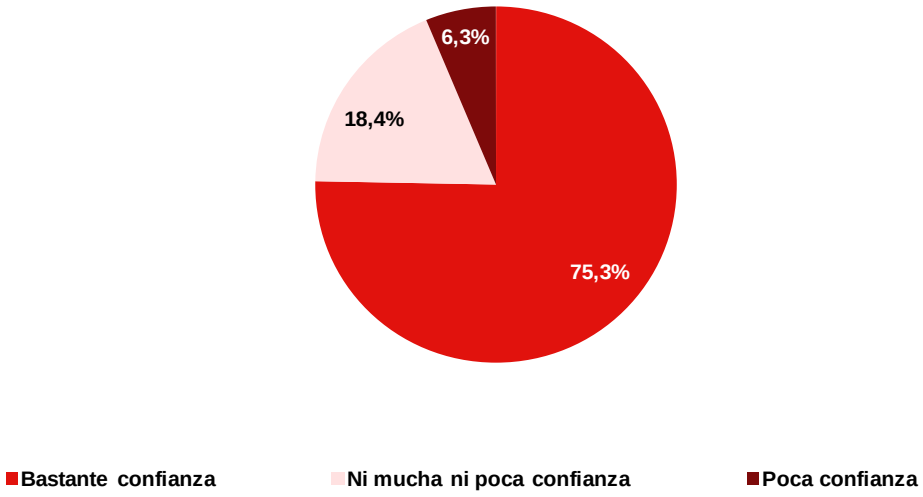
Grado de confianza	Microempresa	Pequeña empresa	Mediana empresa
Bastante confianza	83,4	89,9	93,6
Ni mucha ni poca confianza	16,4	9,8	5,8
Poca confianza	0,2	0,3	0,6

Base: Empresas que utilizan la factura electrónica (n=317) *Fuente: INTECO*

Por último, el análisis se detiene en la confianza que tiene para el colectivo entrevistado la realización de operaciones de **contratación electrónica.** Bajo esta denominación se engloban los procedimientos electrónicos que permiten cumplir las diferentes fases del proceso de contratación de la forma más automatizada posible.

El uso de medios electrónicos en este tipo de procedimientos no está muy extendido (un 17,7% de las empresas dicen hacerlo). No obstante, para aquellas que sí realizan operaciones de contratación electrónica, la confianza que les genera es notable (un 75,3% señala tener bastante confianza).

Gráfico 65: Grado de confianza de las empresas en la contratación electrónica (%)



Base: Empresas que utilizan la contratación electrónica (n=285) *Fuente: INTECO*

Como muestra la siguiente tabla, cuanto mayor es el tamaño de la empresa más elevado es la confianza mostrada por las empresas a la hora de utilizar servicios de contratación electrónica.

Tabla 15: Grado de confianza en la contratación electrónica, según tamaño (%)

Grado de confianza	Microempresa	Pequeña empresa	Mediana empresa
Bastante confianza	74,7	81,8	87,5
Ni mucha ni poca confianza	18,7	14,5	12,5
Poca confianza	6,6	3,7	0,0

Base: Empresas que utilizan la contratación electrónica (n=285) *Fuente: INTECO*

7.2 Frenos al desarrollo de la Sociedad de la Información

La Sociedad de la Información brinda a las empresas múltiples servicios de Internet para facilitar o agilizar sus actividades de negocio, a lo que las empresas responden otorgando una notable confianza en el uso de estos servicios. Sin embargo, todavía existe un camino por recorrer en la generalización de estos servicios.

Para identificar los posibles frenos a la expansión de estos servicios, se analizan las motivaciones que las empresas no usuarias de cada servicio muestran para, precisamente, no utilizar tal servicio. Por tanto, en cada caso se tienen en cuenta únicamente aquellas organizaciones que indicaron previamente que no utilizaban el servicio en cuestión.

Como indica la Tabla 16, las razones difieren en función del servicio analizado.

- Con carácter general, la falta de necesidad o interés son las principales motivaciones aportadas por las empresas, con valores mayoritarios en todos los casos. Este resultado es especialmente elevado en el caso de las redes sociales (88,6%), la venta a través de comercio electrónico (87,0%) y la contratación electrónica (85,8%).

- Con niveles de declaración muy inferiores, el motivo relativo a la incomodidad de uso destacan las empresas que no utilizan los trámites de e-Administración, así como la factura electrónica, o la banca online (16,7%, 15,3% y 12,5% respectivamente).

- La falta de conocimientos sobre el uso presenta en todos los casos valores por debajo del 10%: es el principal motivo para un 9,3% de las organizaciones que no utilizan firma electrónica y para un 7% de las no son clientes de banca en línea.

- La falta de seguridad es un motivo alegado de forma minoritaria, si bien destaca que un 12,5% de las empresas que no son usuarias de banca online apuntan esta respuesta y un 7,7% en el caso de compra online.

Más allá de estos valores, sorprende que los responsables de seguridad de las empresas que han participado en las entrevistas en profundidad apunten de forma mayoritaria a la falta de concienciación y formación para no utilizar los distintos servicios TIC. En su opinión, la costumbre impera en la operativa diaria: si algo ha funcionado hasta ahora, no busco otras alternativas. En todo caso, consideran que Internet es imprescindible para las empresas, puesto que ofrece ventajas para el negocio y para aquellas que no utilizan la Red supone un lastre a la hora de competir.

Tabla 16: Motivos por los que las empresas no utilizan los servicios ofrecidos Internet (%)

Servicios	% empresas que no utilizan	Motivos				
		No necesita/No interesa	No sabe cómo usarlo	No le parece seguro	Le resulta incómodo	No sabe / no contesta
Venta a través de Internet	84,9%	**87,0**	3,4	3,7	5,9	-
Contratación electrónica	78,0%	**85,8**	6,0	2,2	6,0	-
Factura electrónica	77,7%	**77,7**	6,2	0,8	**15,3**	-
Perfil en redes sociales	71,4%	**88,6**	4,6	3,3	3,5	-
Firma electrónica (Certificado, DNI electrónico, etc.)	56,9%	**82,4**	**9,3**	1,9	6,4	-
Compra a través de Internet	54,7%	**82,4**	3,5	**7,7**	6,4	-
Trámites con la administración (e-Administración)	44,2%	**74,2**	6,3	2,8	**16,7**	-
Página web empresarial	44,3%	**86,3**	4,4	1,1	1,6	6,6
Banca electrónica/medios de pago online	28,4%	**68,0**	**7,0**	**12,5**	**12,5**	-

Fuente: INTECO

8 PERFILES DE SEGURIDAD Y CONTINUIDAD DE NEGOCIO EN LA EMPRESA

El establecimiento de perfiles diferenciados de empresas en base a técnicas estadísticas multivariantes permite aportar un análisis más profundo de los resultados mostrados en los apartados anteriores.

El análisis clúster o de conglomerados es una técnica de análisis multivariante que permite clasificar una población amplia (las organizaciones participantes en el estudio) en grupos, de forma que el grado de similitud entre los miembros de un mismo perfil es mayor que el grado de asociación entre miembros de grupos diferentes. Cada perfil se describe en función de las características de los miembros que lo componen.

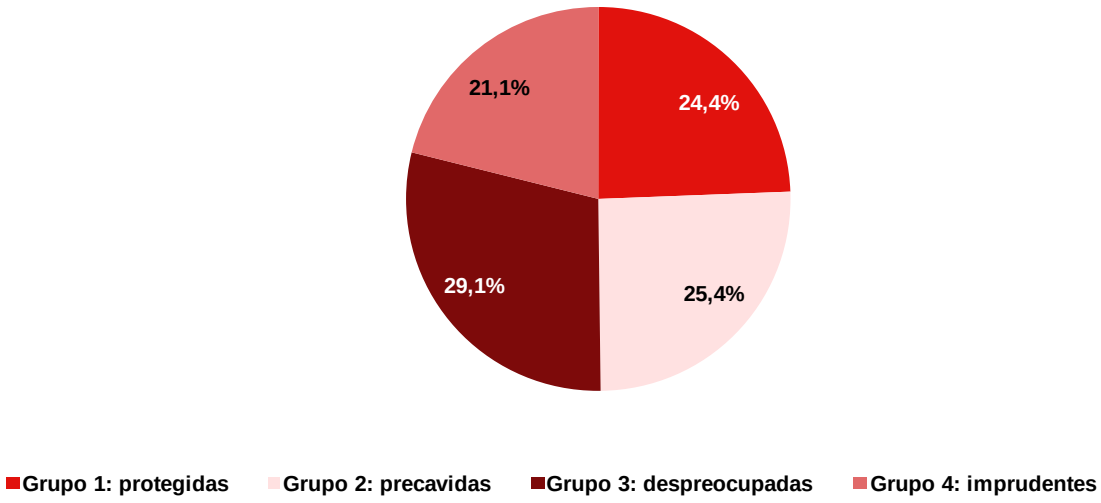
El objetivo perseguido con la aplicación del análisis clúster ha sido por un lado, ordenar los datos obtenidos en los análisis previos, así como confeccionar grupos de empresas que orienten en la toma de decisiones, teniendo en cuenta la información disponible en el análisis.

En este estudio se han realizado dos análisis de este tipo, obteniendo 4 grupos diferenciados respecto a la percepción de la seguridad de la información y la e-confianza y 4 respecto a la continuidad de negocio en la pequeña y mediana empresa.

8.1 PERFILES RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN Y E-CONFIANZA

El primer análisis clúster en base a la percepción de la seguridad y la e-confianza ha permitido obtener cuatro grupos diferenciados de empresas, denominadas de forma simbólica como protegidas, precavidas, despreocupadas e imprudentes. Como muestra el siguiente gráfico, la distribución en los cuatro grupos es bastante homogénea.

Gráfico 66: Distribución de empresas según sus perfiles de seguridad y e-confianza (%)



Base: Total empresas que responden al cuestionario de seguridad (n=1.144) *Fuente: INTECO*

Las principales características de cada grupo se resumen en la siguiente tabla.

Tabla 17: Perfiles de empresas sobre seguridad de la información y e-confianza

	Perfil 1: Empresas "protegidas"	Perfil 2: Empresas "precavidas"	Perfil 4: Empresas "despreocupadas"	Perfil 3: Empresas "imprudentes"
Sector	Industria y servicios a empresas	Todos los sectores	Comercio y hostelería	Comercio y hostelería / Otros servicios
Tamaño	Predominio de medianas empresas	Predominio de microempresas	Predominio de microempresas	Predominio de micro y pequeñas empresas
Protección en materia de seguridad	Elevada preocupación por la seguridad de la información. Cuentan con medios técnicos y humanos para garantizarla	Elevada de preocupación por la seguridad de la información, aunque no siempre cuentan con los mejores medios técnicos.	Escasa preocupación por la seguridad de la información	Escasa preocupación por la seguridad de la información. No es prioritaria.
Incidentes de seguridad	Baja incidencia de situaciones de riesgos.	Baja incidencia de situaciones de riesgo.	Baja incidencia de situaciones de riesgo.	Alta incidencia de situaciones de riesgo. Tres de cada diez empresas han sufrido incidentes de seguridad en el último año.
E-confianza	Grado de confianza en Internet alto.	Grado de confianza en Internet medio/alto. Utilización muy escasa.	Grado de confianza en Internet medio. Baja utilización de servicios de Internet.	Grado de confianza en Internet medio/alto. Elevado uso de TIC.

Fuente: INTECO

A continuación, se hace una descripción de los diferentes perfiles. El análisis de cada grupo se presenta articulado en base a los siguientes aspectos:

- El grado de protección en seguridad, a partir de las herramientas, buenas prácticas y políticas de seguridad que las empresas de cada perfil afirman disponer.
- Los incidentes de seguridad que han impactado en la seguridad y/o en la continuidad de las actividades de la empresa.
- El grado de e-confianza en la utilización de los diferentes servicios de Internet.

8.1.1 Perfil 1: Empresas "protegidas"

Las empresas incluidas en el grupo 1 se denominan "protegidas", puesto que integran la seguridad de la información a nivel técnico y organizativo. Este grupo está formado por las empresas de mayor tamaño y de los sectores industrial y de servicios empresariales. Además se caracterizan por su alto grado de incorporación de TIC (ordenadores de sobremesa, ordenadores portátiles y smartphones) en comparación con el resto de grupos.

Protección en materia de seguridad

Las empresas "protegidas" presentan un nivel elevado de preocupación por la seguridad de la información, y cuentan con medios técnicos y humanos para garantizarla. Ello se comprueba, entre otros, por los siguientes aspectos:

- Afirman disponer de herramientas y recursos humanos dedicados a la seguridad en mayor medida que el resto de perfiles.
- Aplican mayoritariamente prácticas de seguridad destinadas a los empleados, como la utilización de herramientas de filtrado y contraseñas para acceder a equipos y documentos.
- La importancia por la seguridad se refleja en el establecimiento de acciones planificadas, como la realización periódica de auditorías de seguridad en 1 de cada 3 empresas. Además, la dirección de las empresas protegidas otorga mucha importancia a la seguridad de la información (por encima del 8, en una escala de 1 a 10).

Incidentes de seguridad

La incidencia de riesgos de seguridad es inferior al dato para el conjunto de empresas (un 21,9% frente a un 26,1%), si bien se muestran más proactivos a la hora de combatir estos incidentes.

- El malware, los emails masivos publicitarios y los fallos técnicos son los incidentes de seguridad más declarados por las empresas "protegidas".
- Tras sufrir un incidente, son las empresas de este perfil las que señalan en mayor medida actualizar y adoptar nuevas herramientas y medidas de seguridad.

E-confianza

De forma general, su grado de confianza en los servicios de Internet es alto. Así, utilizan mayoritariamente la banca electrónica y los medios de pago online, los trámites con la e-administración y la firma electrónica. También destacan en la disponibilidad de página web y en la compra online. Por último, encabezan la utilización de servicios más minoritarios, como la factura electrónica y se muestran todavía reticentes a utilizar redes sociales.

8.1.2 Perfil 2: Empresas "precavidas"

El segundo grupo integra mayoritariamente a microempresas a las que se ha otorgado la denominación de "precavidas" ya que, reconociendo un nivel bajo de incidencias de seguridad, muestran una gran preocupación por la seguridad de la información.

Protección en materia de seguridad

Las empresas "precavidas" cuentan tanto con medios técnicos como humanos para garantizar la seguridad de la información, como lo demuestran las siguientes características:

- Disponen de herramientas destinadas a proteger sus equipos y sistemas en mayor medida que el resto de perfiles, especialmente en lo referente a las soluciones paquetizadas.
- Cuentan con personal dedicado a la seguridad de la información, ya sea interno o externo.
- Hacen copias de seguridad de los datos y realizan actualizaciones del sistema operativo o de los programas en mayor medida que las empresas "despreocupadas" y las denominadas como "imprudentes".

Incidentes de seguridad

La incidencia de situaciones de riesgo presenta en este grupo, junto con las empresas "despreocupadas", los niveles más bajos.

Los incidentes más comunes percibidos por las empresas de este grupo son los e-mails masivos publicitarios y el malware.

E-confianza

A pesar de utilizar los servicios de Internet en una proporción reducida con respecto al total, el grado de confianza que depositan en los mismos es medio/alto.

8.1.3 Perfil 3: Empresas "despreocupadas"

El grupo de empresas "despreocupadas" recibe esta denominación por el reducido nivel de incorporación de equipamiento TIC y el correspondiente menor peso de los aspectos de seguridad.

Principalmente integra a microempresas, mayoritariamente de comercio y hostelería. Se trata, por tanto, de autónomos y de pequeñas empresas de servicios de proximidad.

Protección en materia de seguridad

A excepción del antivirus, herramienta de uso generalizado en los negocios españoles, el grueso de herramientas y medidas de seguridad disponible en las empresas de este perfil muestra una penetración sensiblemente inferior con respecto al resto de grupos.

Incidentes de seguridad

El escaso nivel de equipamiento TIC y la escasa preparación en materia de seguridad de las empresas "despreocupadas" puede ser la razón de que la percepción de haber sufrido incidentes en el último año sea también baja.

E-confianza

Al igual que muestran un reducido uso de equipamiento TIC, las empresas del grupo 3 aprovechan tímidamente las posibilidades de los servicios de Internet. En este sentido, su nivel de e-confianza también es el más bajo de los diferentes *clústeres*, aportando motivos como la no necesidad de los servicios o también el desconocimiento o la percepción de que no son seguros.

8.1.4 Perfil 3: Empresas "imprudentes"

Este grupo está integrado por las llamadas "imprudentes", ya que teniendo un nivel de equipamiento TIC mayor que otros grupos, no muestran una apuesta clara por la seguridad de la información.

Se trata, en gran medida de empresas pertenecientes a los sectores de comercio y hostelería y de otros servicios. Existe mayor presencia de pequeñas empresas que en los grupos denominados como "precavidas" y "despreocupadas".

Protección en materia de seguridad

Los medios técnicos y humanos dedicados a la seguridad de la información disponibles en las empresas "imprudentes" son, en general, inferiores a los datos ofrecidos a nivel general:

- Estas empresas cuentan con herramientas de seguridad en menor medida que las "protegidas" y "precavidas".
- En cuatro de cada diez empresas no está considerado el personal dedicado a la seguridad informática (frente a un 56,3% a nivel global), y entre las que sí cuentan con él la gran mayoría lo hace mediante una empresa externa.
- En 8 de cada 10 empresas no existe ningún tipo de restricción de acceso a Internet, dato que indica menor grado de incorporación de esta buena práctica que el resto de *clústeres*.

Incidentes de seguridad

En este grupo se ha detectado una mayor proporción de incidentes de seguridad, frente a los que han reaccionado utilizando en mayor medida las diversas alternativas disponibles.

- El malware, los e-mails masivos publicitarios y el fraude online/phishing son los sucesos más frecuentes.
- Junto con la instalación de herramientas y nuevas medidas de seguridad, las empresas "imprudentes" utilizan otras alternativas para combatir un incidente, como la impartición de formación específica o la incorporación de medidas de continuidad de negocio.

E-confianza

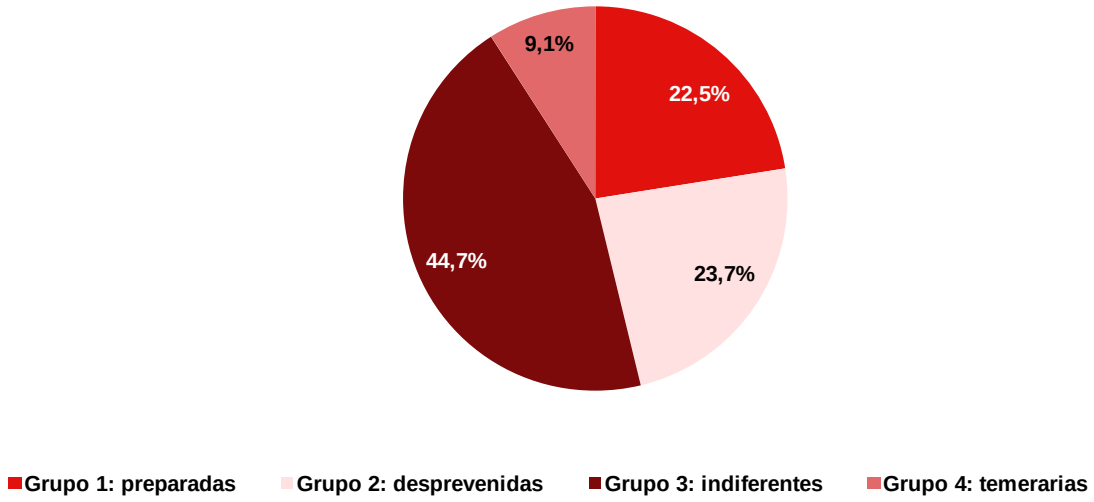
Su grado de confianza en los medios de Internet es medio/alto, y los utilizan especialmente para promocionarse y comercializar sus productos y servicios. Destaca el nivel de uso de servicios como la página web empresarial, las redes sociales o la compra y la venta a través de comercio electrónico, superior al del resto.

8.2 PERFILES RELACIONADOS CON LA CONTINUIDAD DE NEGOCIO

El segundo análisis de conglomerados o *clúster* se basa en la percepción de las empresas respecto a aspectos de continuidad de negocio. En este caso, se han obtenido cuatro grupos de empresas diferenciados, denominados de forma intuitiva como "previsoras", "confiadas", "indiferentes" y "temerarias" (ordenados de menos a más según su situación de riesgo potencial)

El Gráfico 68 muestra la distribución en los cuatro grupos, siendo las empresas indiferentes las que mayor presencia tienen (un 44,7%), seguidas de las preparadas y desprevenidas con una proporción similar (un 22,5% y un 23,7%, respectivamente). El grupo más minoritario es el de las empresas "temerarias" (9,1%).

Gráfico 67: Distribución de las empresas en función de su perfil en materia de continuidad de negocio (%)



Base: Total empresas que responden a la parte de CN (n=1.109) *Fuente: INTECO*

Como aproximación, se resumen en la siguiente tabla las principales características de cada grupo.

Tabla 18: Perfiles o grupos de empresas. Continuidad de negocio en la empresa

	Perfil 1: Empresas "preparadas"	Perfil 2: Empresas "desprevenidas"	Perfil 3: Empresas "indiferentes"	Perfil 4: empresas "temerarias"
Sector	Sector servicios	Sector comercio y hostelería	Sector industria y sector comercio y hostelería	Sector industria
Tamaño	Medianas y pequeñas empresas	Pequeñas y micro empresas	Microempresas	Microempresas
Incidencias	Existencia de incidentes baja. Están identificadas las actividades críticas de negocio. Con estrategia para situaciones de crisis / desastre. Dicen estar bien preparadas para afrontar una situación de crisis.	Existencia de incidentes alta. No están identificadas las actividades críticas de negocio. Con estrategia para situaciones de crisis / desastre. Dicen estar medianamente preparadas para afrontar una situación de crisis.	Existencia de incidentes baja. No están identificadas las actividades críticas de negocio. Sin estrategia para situaciones de crisis / desastre. Dicen no estar preparadas para afrontar una situación de crisis.	Existencia de incidentes alta. No están identificadas las actividades críticas de negocio. Sin estrategia para situaciones de crisis / desastre. Dicen estar poco preparadas para afrontar una situación de crisis
Conocimiento e implementación del PCN	Conocen los PCN y tienen implementadas medidas frente a contingencias (BCP) y de recuperación ante desastres técnicos (DRP)	Conocen los PCN y tienen implementadas medidas de recuperación ante desastres técnicos (DRP)	No conocen PCN y no tienen implementadas medidas de recuperación.	No conocen PCN y no tienen implementadas medidas de recuperación.

Fuente: INTECO

A continuación, se hace una descripción de los diferentes perfiles. El análisis de cada grupo se presenta estructurado en función de los siguientes aspectos:

- Incidencias que pondrían en peligro la continuidad del negocio y actividades críticas.
- Conocimiento e implementación del Plan de Continuidad de Negocio

8.2.1 Perfil 1: Empresas "preparadas"

El primer grupo está integrado por empresas que se caracterizan por su proactividad, a la hora de establecer estrategias de continuidad de negocio y reaccionar frente a incidentes.

En este grupo existe un mayor porcentaje de pequeñas y medianas empresas que en el resto de perfiles de continuidad de negocio. Además, está constituido por compañías de servicios, tanto empresariales como otros servicios personales.

Incidencias que pondrían en peligro la continuidad del negocio y actividades críticas

Las empresas preparadas apenas han sufrido algún incidente grave durante el último año, aunque muestran una preocupación elevada por la posibilidad de que exista alguna. Se caracterizan entre otras cuestiones porque:

- Tres de cada cuatro empresas han identificado las operaciones o actividades críticas de negocio, en contraste con el resto de grupos.
- Son las que se sienten más y mejor capacitadas para afrontar situación de crisis, desastre o contingencia.
- Dos de cada tres empresas preparadas disponen de estrategias de continuidad de negocio, proporción muy superior al resto de grupos. Entre las razones para no disponer de estas medidas se señalan, además de la falta de necesidad, el coste excesivo, el desconocimiento o la existencia de otras prioridades de seguridad.

Conocimiento e implementación del Plan de Continuidad de Negocio

El clúster de empresas preparadas se sitúa igualmente a la cabeza en cuanto a conocimiento declarado de los Planes de Continuidad de Negocio e implantación en la empresa de planificaciones que abarcan globalmente la continuidad.

8.2.2 Perfil 2: Empresas "desprevenidas"

Las empresas "desprevenidas" son aquellas que habiendo sufrido incidentes que podrían poner en riesgo la continuidad de sus operaciones, no apuestan claramente por establecer estrategias proactivas.

El segundo grupo comprende principalmente las empresas de comercio y hostelería y está compuesto por un mayor porcentaje de pequeñas y medianas empresas que en el resto de clústeres.

Incidencias que pondrían en peligro la continuidad del negocio y actividades críticas

Las empresas "desprevenidas" han sufrido incidentes de seguridad en el último año aunque su comportamiento a la hora de protegerse frente a estos sucesos no es tan proactivo como el mostrado por las "preparadas". Entre otras cuestiones se caracterizan por:

- Haber sufrido incidencias durante el último año, principalmente tecnológicas (energía, climatización, sistemas o aplicaciones informáticas, etc.), destacando también los ataques de seguridad de la información.
- Cerca de un tercio de las empresas tiene identificadas las actividades cuyo fallo o interrupción impactaría en su negocio, asemejándose a las empresas "indiferentes" y "temerarias".
- Las "desprevenidas" sienten que tienen una preparación similar a las "indiferentes", aunque se diferencian de estas en que más de la mitad de las empresas inmunes afirman que disponen de procedimientos para hacer frente a desastres o contingencias, o lo tienen previsto.

- Destacan las empresas que desconocen la razón para no haber previsto una estrategia de este tipo, así como las que indican que no disponen de tiempo o recursos.

Conocimiento e implementación del Plan de Continuidad de Negocio

Como ocurre con las empresas "indiferentes" una proporción notable de empresas "desprevenidas" no conoce qué conlleva un PCN. Por último, menos de un cuarto de las empresas disponen de un plan que garantice el restablecimiento de las operaciones críticas de negocio (o al menos la parte tecnológica) en caso de desastre o crisis.

8.2.3 Perfil 3: Empresas "indiferentes"

Las empresas incluidas en el tercer perfil se denominan "indiferentes", ya que se caracterizan por no mostrar una gran preocupación por los incidentes que pudieran afectar a la continuidad de su negocio ni por las consecuencias de estos.

Este grupo está formado en su mayoría por microempresas, existiendo una mayor presencia de organizaciones pertenecientes al sector comercio y hostelería y al sector industrial en el conjunto de las de las empresas.

Incidencias que pondrían en peligro la continuidad del negocio y actividades críticas

Las empresas "indiferentes" no se sienten amenazadas por la posibilidad de que exista una incidencia de seguridad que pueda irrumpir en las operaciones críticas, como se deduce de los siguientes aspectos:

- No han percibido en el último año ningún incidente que pudiera poner en riesgo la continuidad del negocio.
- Apenas la cuarta parte tiene identificadas las operaciones o actividades críticas de negocio.
- Tres de cada cuatro empresas "indiferentes" se sienten preparadas para afrontar una contingencia grave.
- Tres cuartas partes no ha previsto alguna estrategia o procedimiento de reacción en caso de desastre. La razón que esgrimen es que creen que la probabilidad de que ocurra un impacto es muy reducida.

Conocimiento e implementación del Plan de Continuidad de Negocio

Este grupo se muestra desconocedor del concepto de Plan de Continuidad de Negocio en mayor proporción que el resto. En este sentido, una proporción notable de empresas "indiferentes" alega que no dispone de medidas de continuidad de negocio porque son innecesarias.

8.2.4 Perfil 4: Empresas "temerarias"

Por último, existe un grupo de empresas que se diferencian por declararse peor preparadas que el resto y disponer de escasos recursos para hacer frente a los incidentes que sufren, por lo que se han denominado "temerarias".

El cuarto grupo analizado se compone de microempresas, principalmente industriales.

Incidencias que pondrían en peligro la continuidad del negocio y actividades críticas

Las empresas "temerarias" han sufrido incidentes al igual que las "desprevenidas", si bien son conscientes de su baja preparación y protección, motivada por la falta de recursos. Entre otras características, destacan las siguientes:

- Estas empresas han sufrido distintos incidentes en el último año, mayoritariamente relativos a la falta de suministro por parte de los proveedores, lo que las diferencia de las desprevenidas.
- A pesar de las posibles consecuencias de estos incidentes, este grupo es el que identifica en menor medida las actividades críticas para que su negocio no se interrumpa.
- Asimismo, destacan por sentirse peor preparadas que el resto de empresas para hacer frente a una situación de crisis o desastre.
- Este hecho se demuestra en la escasa previsión de estrategias para hacer frente a estos acontecimientos. Sin embargo, son las que más argumentan razones relativas a la falta de tiempo o recursos para abordar cuestiones de continuidad.

Conocimiento e implementación del Plan de Continuidad de Negocio

En línea con las empresas "desprevenidas", los Planes de Continuidad de Negocio son desconocidos para una proporción importante de empresas "temerarias". Asimismo, el grado de implantación de medidas y procesos que permitan recuperar las actividades críticas de negocio, o al menos la parte tecnológica, es bajo.

9 CONCLUSIONES

En el presente epígrafe se resumen las conclusiones del presente estudio, en las que se contrasta la situación interna percibida por la micro, pequeña y mediana empresa española en relación a sus puntos fuertes y débiles en materia de seguridad de la información y continuidad de negocio, así como con los factores externos asociados. Estas conclusiones constituyen la base para la posterior formulación de recomendaciones dirigidas a la pequeña y mediana empresa, a los fabricantes de soluciones de seguridad y a las Administraciones Públicas.

De este modo, las principales conclusiones del informe tratan de responder a los siguientes interrogantes: ¿cuál es la situación de la empresa española para afrontar incidentes de seguridad de la información? Y, en consecuencia, ¿qué actuaciones deberían emprenderse para afrontar con éxito la protección efectiva de los activos de información de la empresa?

9.1 PUNTOS DÉBILES

1) Falsa sensación de seguridad en la empresa

Una de las declaraciones extraídas de las entrevistas a los responsables de seguridad de las empresas es la percepción de que los ataques de seguridad de la información están dirigidos a grandes compañías o entidades, por lo que no es una preocupación real para las empresas pequeñas.

De igual forma, creen que la posibilidad de sufrir un incidente grave es remota y por tanto, que no necesitan disponer de procedimientos que permitan recuperar la actividad en caso de desastre.

Sin embargo, como indica la industria de seguridad, 2011 se caracteriza por ser el año de los ciberataques[33]. En este panorama influye de forma notable que los atacantes se sirven de la tecnología para mejorar las fórmulas de ataque y perfeccionar el malware, con el objetivo de provocar el mayor impacto para la víctima, tanto en términos económicos, como operacionales o incluso reputacionales.

Por tanto, esta percepción evidencia un desconocimiento de los riesgos existentes y de los procesos de gestión asociados, así como de la funcionalidad que aportan las medidas, prácticas y procedimientos de protección y continuidad de negocio y, en consecuencia, la posición de mayor vulnerabilidad en el caso de incidente.

2) Deficiencias en la cultura de seguridad en las empresas

Los profesionales en seguridad de la información que han participado en el grupo de expertos están de acuerdo al afirmar que es necesario avanzar en la incorporación de la cultura de la seguridad de la información y la continuidad de negocio como parte fundamental de la estrategia de la empresa.

[33] Fuente: PANDALABS (2011) *Informe anual. Resumen 2011*. Disponible en: http://pandalabs.pandasecurity.com/es/informe-anual-pandalabs-2011/.

Entre otras razones, las empresas manejan a diario gran cantidad de información y parte de esta información es más sensible, ya que es estratégica para el negocio, contiene datos personales de clientes, proveedores o empleados, incluye referencias de propiedad intelectual, etc. Tanto para asegurar su actividad como para cumplir con los requisitos legales de aplicación, es imprescindible la adecuada gestión de la información.

Sin embargo, el enfoque en la seguridad y continuidad de negocio no siempre está presente en la estrategia empresarial de la organización y los empresarios y gestores, a pesar de percibir la importancia de estas áreas, no disponen de formación suficiente en gestión de la seguridad.

3) El menor tamaño resulta un factor determinante (en negativo) del nivel de protección

A lo largo del estudio se constata la heterogeneidad de las organizaciones, lo que implica unas necesidades específicas según el tamaño, madurez y sector de actividad de cada una de ellas. Las empresas de mayor tamaño y recursos son las que declaran un mayor nivel de adopción de medidas, hábitos y procedimientos de protección de la infraestructura TI y de continuidad de las actividades en caso de desastre.

Asimismo, las micro y pequeñas empresas perciben que su falta de recursos y tiempo les empuja a no considerar en ocasiones, aspectos relevantes y necesarios. También es frecuente que no dispongan de personal especializado en seguridad de la información.

4) Escaso margen en el tiempo de interrupción permitidos

Casi dos de cada tres empresas que participan en el estudio perciben que no se pueden permitir parar la actividad durante más de un día, puesto que esta paralización acarrearía grandes pérdidas e incluso, situaciones irreversibles.

5) Enfoque de la seguridad excesivamente enfocado a la dimensión tecnológica

Otra de las debilidades observadas en la empresa se refiere a la consideración de la protección únicamente desde el punto de vista del componente tecnológico. Así, el colectivo participante en el estudio muestra una notable adopción de herramientas de seguridad, pero todavía existe margen de mejora en cuanto a la incorporación y perfeccionamiento de buenas prácticas y estrategias que aseguren la recuperación de la actividad en caso de desastre, incluyendo aspectos no sólo tecnológicos, sino también organizativos, reputacionales, etc.

Para ello, la implementación de Sistemas de Gestión de la Seguridad de la Información (SGSI) en base a la norma ISO 27001 obliga a tener en cuenta una visión global sobre el estado de seguridad de los sistemas de información. Además, la certificación permite a las organizaciones proporcionar unas garantías de cumplimiento respecto a los servicios ofrecidos.

9.2 PUNTOS FUERTES

1) Buena capacidad tecnológica de la empresa

Las pequeñas y medianas empresas participantes en el estudio reflejan la situación actual en cuanto a nivel de incorporación de las TIC: ordenadores, equipos portátiles y dispositivos móviles

son herramientas imprescindibles para la actividad empresarial. Además, las empresas asumen la renovación de estos equipos como un factor que influye en los negocios.

Por su parte, Internet ofrece numerosas posibilidades y servicios de apoyo para la gestión y desenvolvimiento de la actividad, por lo que su uso está muy extendido entre el tejido empresarial.

En el presente estudio, se corrobora un notable nivel de e-confianza en la adopción de servicios de la Sociedad de la Información. La banca electrónica y los medios de pago online, los trámites con la e-Administración o el negocio electrónico son parte de los servicios electrónicos utilizados diariamente.

2) Notable nivel de implantación de medidas de seguridad preventivas

Hoy en día, las empresas disponen en el mercado numerosas soluciones de seguridad que les ofrecen diversas funcionalidades de prevención contra incidentes de seguridad. Herramientas como los programas antivirus y cortafuegos están ampliamente extendidos y normalmente, junto con estos, los paquetes de seguridad suelen incluir otras funcionalidades avanzadas, como el bloqueo de ventanas emergentes, los filtros antispam o herramientas para el cifrado de datos.

Por tanto, la situación de base en cuanto a la protección de la información es favorable para la incorporación progresiva de medidas y procesos de gestión de la continuidad que impliquen la consideración de la seguridad como parte de la estrategia empresarial.

3) Sensibilidad al tiempo de reactivación

El margen de tiempo para reactivar la actividad en caso de desastre identificado por las empresas constituye un punto de partida positivo respecto de la importancia que le dan a estar preparadas para afrontar situaciones de irrupción de la actividad.

4) Respuesta favorable a iniciativas

Las empresas se relacionan y colaboran estrechamente con diferentes agentes en su día a día: Administraciones Públicas, organizaciones empresariales, colegios profesionales, etc.

Estos actores canalizan diferentes iniciativas de concienciación y sensibilización orientadas a mejorar la gestión para la pequeña y mediana empresa, a las que estas suelen responder activamente. Así, por ejemplo, en 2009 INTECO llevó a cabo el Programa de impulso a la implantación y certificación de Sistemas de Gestión de Seguridad de la Información, SGSI (ISO 27001) en la pequeña y mediana empresa española, en el que se certificaron 143 empresas, logrando posicionar a España entre los países del mundo con más implantaciones de ISO 27001.

9.3 AMENAZAS

1) Lento progreso de la seguridad

La comparación con informes previos de INTECO indica que no se ha producido un avance claro en materia de seguridad y continuidad de negocio en el colectivo empresarial en los últimos tres años. Este factor puede implicar una pérdida de competitividad de la pequeña y mediana empresa.

Los expertos señalan que es imprescindible avanzar en la concienciación para promover procesos de reflexión en la organización y establecimiento de estrategias que permitan incrementar progresivamente el nivel de protección y su resistencia ante impactos.

2) Recrudecimiento de las consecuencias de los ataques

La industria de seguridad trata de concienciar del avance de la ciberdelincuencia y de la profesionalización de los ataques. Hoy en día cualquier organización puede ser víctima de un ataque de seguridad, puesto que la información de las organizaciones resulta muy lucrativa si cae en manos de terceros malintencionados.

A ello contribuye el desarrollo tecnológico, que permite perfeccionar las técnicas y generar nuevas variantes de código malicioso. A partir de este perfeccionamiento, lanzan ataques específicamente diseñados para empresas o sectores en concreto. Las consecuencias de estos ataques son superiores y no afectan solo a la parte operativa y sino que son también económicas, de reputación, etc.

3) Nuevos desafíos tecnológicos y nuevos riesgos de seguridad

El desarrollo de nuevas tecnologías como los dispositivos móviles avanzados (Smartphones, tabletas, etc.) o los nuevos servicios en modo cloud computing (sobre todo en las modalidades *Software as a Service*) aportan nuevas funcionalidades a las empresas y estas se están beneficiando de características como la movilidad, la escalabilidad del servicio o el ahorro económico, entre otras.

Sin embargo, junto con los beneficios también aparecen nuevas amenazas, que no siempre solucionan las herramientas de seguridad de que disponen las empresas. Por tanto, debe realizarse un esfuerzo paralelo para la incorporación de medidas de protección adicionales que aporten una cobertura suficiente.

En este sentido, los proveedores de estas nuevas tecnologías y la industria de seguridad deben promover el desarrollo de soluciones específicas de protección y desplegar una labor de asesoramiento a las pequeñas y medianas empresas para el correcto aprovechamiento de las mismas.

9.4 OPORTUNIDADES

1) Enfoque conjunto de los diferentes actores para una mejor orientación hacia las pequeñas y medianas empresas

Una de las principales conclusiones extraídas del grupo de expertos realizado en el marco del estudio apunta a la necesidad de avanzar en la concienciación y en la formación en materia de seguridad de la información y la continuidad de las operaciones.

En este sentido, existen multitud de actores (industria de la seguridad, organizaciones empresariales, administraciones públicas, etc.) orientados a prestar servicio a las pequeñas y medianas empresas, en función de las necesidades concretas de este colectivo en cada momento.

La adecuada planificación de los esfuerzos desplegados por estos actores permite aprovechar sinergias y contribuir efectivamente a mejorar la sensibilización de este colectivo por la protección de la información e implicar a las mismas en el aumento de la concienciación y formación interna.

2) Amplia cartera de servicios de seguridad y continuidad de negocio

En cuanto a las soluciones incorporadas por las empresas, los expertos señalan que se debe producir un avance en la adaptación de las mismas a la realidad concreta de cada empresa.

Actualmente, son varias las posibilidades existentes en el mercado de la seguridad de la información: soluciones de software y hardware de seguridad, servicios de consultoría, certificación, auditoría, formación, etc.

La empresa debe asumir la seguridad de la información como la suma de estos elementos. Para lograrlo, la colaboración de los agentes mencionados es indispensable, en el sentido de proporcionar soluciones integrales, colaborativas, escaladas y asumibles por los responsables de seguridad de las empresas (en muchos casos, los responsables de TI o incluso los propios empresarios o gerentes).

3) Externalización de las funciones de TI y seguridad de la información

En el presente informe se muestra cómo las empresas de menor tamaño externalizan las funciones de TI y seguridad a profesionales especializados. Con ello, las empresas perciben que emplean mejor sus recursos internos, a la vez que disponen de un profesional externo con un conocimiento más profundo y actualizado.

La oportunidad radica en el servicio que presta el profesional externo, puesto que se podría complementar la mera actuación sobre la infraestructura de TI de la empresa con acciones informativas sobre la evolución de la seguridad, novedades en cuanto a riesgos y nuevos servicios, o fórmulas de mejora en la externalización.

Esta actuación, en todo caso, debe promover el efectivo control de la empresa en la seguridad de los sistemas de información y el aumento del nivel de concienciación en materia de protección y continuidad de negocio.

10 RECOMENDACIONES DE ACTUACIÓN

A continuación se presentan las recomendaciones extraídas de los resultados y conclusiones del estudio, diferenciando entre las dirigidas a las empresas, a la industria de seguridad de la información y a la Administración Pública.

10.1 RECOMENDACIONES PARA LA MICRO, PEQUEÑA Y MEDIANA EMPRESA

1) Avanzar en la sensibilización de las empresas sobre seguridad de la información.

Tal como se señalaba por los expertos en seguridad de la información que participaban en el estudio, el talón de Aquiles de las pequeñas y medianas empresas españolas en materia de seguridad de la información es la falta de sensibilización y concienciación en la organización por estos aspectos, lo que se refleja en la falsa percepción de seguridad que existe entre este colectivo, posición que les hace más vulnerables a ataques.

En el sentido de la falta de cultura empresarial, es fundamental el compromiso de la dirección para impulsar dentro de la organización las actividades de gestión de la seguridad de la información y el establecimiento y mejora constante en los aspectos de continuidad de de negocio. Frente a un colectivo empresarial caracterizado en muchos casos por el pequeño tamaño de la actividad y el carácter familiar del negocio, es necesario incidir en la importancia de realizar un proceso de reciclaje interno.

Para ello, deben abordarse las siguientes acciones:

- La dirección debe adquirir los conocimientos básicos de la gestión de la seguridad de la información en la empresa, como parte de sus habilidades directivas. Asimismo, es tarea de los responsables de la empresa promover el alineamiento de los objetivos de la organización con la estrategia de seguridad y continuidad de negocio.

- El departamento o responsable de TI de la empresa debe contar con los conocimientos necesarios para diseñar una estrategia de gestión de la seguridad y consensuarla con la dirección.

2) Considerar la seguridad de la información como un todo e integrarla dentro de la organización.

La seguridad de la información debe abordarse como un todo en el que se contemplen soluciones y herramientas de seguridad, pero también buenas prácticas y procedimientos. Desde este punto de vista, se dejaría de considerar la seguridad de la información como actuaciones puntuales y aisladas, relativas a la instalación de una determinada herramienta que, en muchos casos, ni se actualiza (puesto que se presupone automática).

Frente a esta forma de actuar, una adecuada estrategia implica la revisión, adaptación y mejora continua de los aspectos incluidos en la misma, encaminada a minimizar los riesgos conocidos y a afrontar con mayores garantías las posibles amenazas que pueden impactar sobre la empresa.

Además, al establecer la estrategia de seguridad, la empresa está reflejando el uso idóneo de los sistemas de información por parte de los usuarios. Asimismo, esta estrategia posibilita que las empresas sean capaces de:

- Identificar los activos de información del negocio.
- Analizar los riesgos a los que se exponen.
- Asignar los recursos necesarios, tanto económicos, de personal y de medios técnicos.
- Reforzar el negocio asegurando una mayor resistencia frente a posibles impactos.
- Mejorar la posición de la empresa frente a sus competidores.

3) Acudir a profesionales externos que solventen la falta de recursos internos sin renunciar a la seguridad.

Acometer la gestión de la seguridad de la información no es una tarea sencilla, sobre todo para aquellas empresas de menor tamaño, que disponen de recursos más limitados.

Por ello es aconsejable identificar las áreas sobre las que se debe actuar y las tareas que puedan calificarse como sencillas (con objetivos definidos) y por tanto, asumibles por el personal interno. Igualmente, puede ser recomendable confiar en asesores externos especializados que ayuden a complementar y profundizar en el conocimiento necesario, adaptado a la realidad de cada caso.

Una vez establecidas las bases, la gestión de la seguridad y la continuidad de negocio en la empresa deben convertirse en un proceso sistemático de mejora continua.

4) Utilizar correctamente las herramientas y medidas de seguridad.

Como se señala en el informe, las empresas encuentran en el mercado soluciones de seguridad en paquete y con funcionalidades automatizadas en muchos casos. Dentro de estas soluciones se suelen integrar varios módulos de seguridad orientados cubrir necesidades diversas.

Sin embargo, dichas herramientas pierden su utilidad sin un adecuado conocimiento de su funcionamiento y una adaptación clara a las necesidades de la empresa, contemplando toda la infraestructura de TI de la empresa, incluidos los dispositivos móviles, cada vez más presentes en los negocios.

Así, la mayoría de las empresas es consciente de que dispone de un antivirus y en una notable proporción, de cortafuegos. Más allá de estas medidas, a juicio de los responsables de seguridad, el desconocimiento o la falsa sensación de no necesitar otras opciones existentes en el mercado (e incluso, incluidas en los paquetes de seguridad por defecto) son motivos para no ampliar la protección. Por tanto, no se saca partido a otras herramientas con usos y funcionalidades específicas, como el cifrado de datos que impide el robo de información en las comunicaciones.

Asimismo, es fundamental proveerse de software bajo licencia, que cumpla todas las garantías de legalidad y originalidad, y que, en caso de existir una vulnerabilidad, permita al profesional de la

empresa disponer de parches de seguridad que solventen el problema de forma rápida. En este sentido, la actualización de programas y sistemas es una práctica básica para evitar fallos ocasionados en la instalación.

5) Fomentar la incorporación de buenas prácticas para los miembros de la organización.

La seguridad de la información en las empresas debe incluir, además de los recursos necesarios, la realización de buenas prácticas que extiendan la seguridad más allá del componente técnico.

En este sentido, la dirección y departamento o personal encargado de la seguridad de la información deben trasladar al conjunto de la organización los conocimientos necesarios para que puedan utilizar los recursos de información de manera constructiva. Estos conocimientos pueden proporcionarse con acciones formativas e informativas impartidas por miembros de la organización o por profesionales y organismos externos.

En esta labor es importante insistir en la adecuada utilización de las medidas y herramientas de seguridad. Por ejemplo, tan importante es la disposición de contraseñas como su gestión adecuada (mediante la actualización periódica, el establecimiento de criterios de creación de contraseñas robustas, etc.). Otro ejemplo es la realización de copias de seguridad, medida ineficaz si no viene acompañada de un conjunto de buenas prácticas, como su actualización periódica y su correcto almacenamiento en soportes y lugares adecuados.

6) Adoptar estrategias de continuidad de negocio.

El objetivo de disponer de una estrategia documentada y procedimentada en relación con la utilización de la infraestructura de TI y la gestión de la información de la empresa es asegurar la continuidad de las operaciones, de tal forma que cada miembro de la organización está concienciado y alineado con las actividades y objetivos de la empresa.

Frente a la percepción de la baja probabilidad de sufrir un incidente que suponga la interrupción del negocio, es importante que la dirección esté concienciada de los riesgos y su probabilidad, las debilidades de la empresa y las operaciones que son vitales para el negocio.

La estrategia puede asumirse de forma gradual, comenzando por tareas sencillas y contando con asesores externos. Un primer paso puede ser la realización de auditorías de seguridad que permitan evaluar el estado de la seguridad de la información y las necesidades del mismo.

En base a estas evaluaciones, se pueden diseñar, corregir, adaptar y actualizar las medidas de seguridad. De tal forma que, de llegar a producirse, se dispondrá de un plan de actuaciones para atajar los riesgos y minimizar las consecuencias.

Además, la elaboración e implementación de una certificación en Sistemas de Gestión de la Seguridad de la Información (en base a la norma ISO/UNE EN 27001) permite a la empresa disponer de los mecanismos necesarios para afrontar los posibles riesgos o contingencias que ocurran. Ello sin contar con la garantía que supone de cara a clientes y usuarios.

7) Establecer criterios de seguridad en las relaciones con los proveedores.

Las empresas en su actividad se apoyan en servicios que les prestan terceras partes y que permiten optimizar sus recursos, como es el caso de los suministros o de soluciones de almacenamiento en modo *cloud computing*, cada vez más presentes en las empresas y entidades españolas. Es decir, que parte de la gestión de la seguridad de la información se delega en dicho proveedor, hasta tal punto que un fallo de seguridad o de otra índole en este nivel de la cadena podría ocasionar un impacto negativo o incluso una interrupción de la actividad de la empresa.

Por ello, se deben definir las actividades necesarias y críticas para el negocio en las que intervenga la acción de estos terceros y establecer criterios que aseguren la disponibilidad de estos servicios. En base a estos criterios, se debe igualmente revisar los acuerdos de nivel de servicio contratados con estos proveedores y adaptarlos a las necesidades concretas de la empresa.

8) Mantenerse actualizados de las novedades en materia de riesgos de seguridad y medidas de protección.

Las amenazas evolucionan constantemente, por lo que es tarea de los responsables de gestión de la seguridad en la empresa mantenerse al día de los principales incidentes y de las soluciones aportadas desde la industria de seguridad.

En este sentido, la suscripción a boletines especializados y foros sobre seguridad de las principales firmas de seguridad es una fórmula sencilla y al alcance de las organizaciones, independientemente de su tamaño. Asimismo, desde las organizaciones y colectivos empresariales se realizan acciones de sensibilización, en ocasiones especializados en un determinado sector o colectivo empresarial.

10.2 RECOMENDACIONES DIRIGIDAS A LA INDUSTRIA DE SEGURIDAD

1) Adecuar la oferta de productos y soluciones de seguridad a la realidad de las empresas españolas.

Como se desprende del estudio, las empresas suelen adquirir soluciones estándares, de tal manera que la implicación de la empresa en el proceso de compra es reducida: se considera la incorporación de estas herramientas como una obligación, más que como una inversión. Más aún, en el caso de las empresas más pequeñas que disponen de un número reducido de equipos, la incorporación de soluciones de seguridad por defecto en los equipos conlleva la percepción de que se ha cumplido con este aspecto.

Para llegar adecuadamente la oferta de seguridad a la diversidad de organizaciones que integran el colectivo de pequeñas y medianas empresas, la industria debe incidir tanto en el producto en sí como en el canal de distribución:

- Establecer fórmulas de evaluación de las necesidades de la empresa en función de su infraestructura de TI y las características de su actividad.

- Ofrecer un producto modulable y adaptado en función del diagnóstico previo.

- Adaptar la interfaz del producto para que sea intuitivo y de fácil comprensión para cualquier tipo de usuario.

- Reforzar la información acerca del producto desde el canal de distribución, mediante la formación de los vendedores, la distribución de carteles informativos y materiales de demostración, etc.

2) Desplegar actuaciones que ayuden a complementar la seguridad en la empresa desde la concienciación y la formación.

Como se ha visto en el estudio, las pequeñas y medianas empresas no suelen disponer de recursos concretos destinados a la seguridad de la información y limitan su actuación a la adquisición de una solución de seguridad o a la adopción de una práctica (creación de contraseñas) de forma puntual. O, en otras palabras, “con una vez es suficiente”. Esto conlleva una percepción errónea del estado de seguridad de las empresas.

Desde la industria de la seguridad de la información se debe adoptar una postura proactiva, en el sentido de considerar su propuesta como algo más que una herramienta o acción concreta. El producto puede complementarse con el envío de boletines informativos con enfoques concretos y diferenciados a responsables TIC y a directivos, de tal forma que la seguridad de la información gane peso en la estrategia de la organización.

Asimismo, el despliegue de acciones de formación y asesoramiento dentro de la organización puede resultar muy beneficioso para las empresas, en cuanto a:

- Evaluar las necesidades de cada caso concreto y su evolución y el correspondiente mantenimiento o reconfiguración de los servicios prestados.

- Proporcionar formación desde la base en seguridad de la información de la empresa, para promover que el conjunto de la organización entienda la importancia de esta área y ayude al cumplimiento de las acciones establecidas por la dirección y el responsable de seguridad.

- Asesorar al responsable de seguridad de la información en cuanto a las actividades críticas de negocio y los riesgos que pueden afectar a la seguridad de la información desde el punto de vista de la continuidad de negocio. Transmitir el funcionamiento y beneficios que aporta un Plan de Continuidad de Negocio.

- Informar sobre novedades en cuanto a estándares, legislaciones e iniciativas desarrolladas por las Administraciones Públicas y los organismos de certificación.

- Asimismo, proporcionar conocimiento en cuanto la seguridad de las tecnologías más novedosas y que ganan peso en las empresas españolas, como los dispositivos móviles avanzados y las soluciones de virtualización y *cloud computing*.

3) Promover la profesionalización de las empresas del canal de distribución de soluciones de seguridad.

La industria de la seguridad debe tomar un papel proactivo en la profesionalización del canal de distribución, puesto que el modelo de negocio de venta de productos de seguridad está cambiando hacia la adquisición online del producto (sobre todo, en el caso de empresas de reducido tamaño), aunque con la necesidad permanente de asesoramiento. Por tanto, es necesario reforzar los procesos pre-venta y post-venta.

El planteamiento de actuaciones por parte de la industria sobre el canal de distribución de productos de seguridad debe partir de la realización de un estudio previo de necesidades de formación de los vendedores en diferentes ámbitos de la seguridad de la información y la continuidad de negocio.

A partir de ese análisis, se aconseja preparar e impartir un programa sectorial de formación adaptado a cada recurso, para que se refuerce el perfil técnico de los profesionales de las empresas de distribución. Los contenidos se deben impartirse en función de los roles y servicios que desempeña cada profesional. Por último, sería aconsejable que estos conocimientos adquiridos pudieran acreditarse por medio de una certificación profesional específica.

4) Colaborar estrechamente con las Administraciones Públicas.

Las Administraciones Públicas conocen la realidad de las micro, pequeñas y medianas empresas españolas, por lo que el establecimiento de colaboraciones público-privadas puede ser muy beneficioso para ambos actores. Así, se podrían destinar recursos y orientar campañas de difusión sectoriales, acuerdos para la realización de acciones específicas en las empresas (como auditorías de seguridad, identificación de actividades críticas y necesidades de negocio, etc.), entre otras.

10.3 RECOMENDACIONES DIRIGIDAS A LA ADMINISTRACIÓN PÚBLICA

1) Asesorar al empresario para que incorpore competencias de seguridad de la información.

A la hora de crear una empresa, se deben establecer canales informativos que proporcionen a los emprendedores los conocimientos u orientaciones necesarias para incorporar la seguridad de la información y la continuidad de negocio como áreas de la estrategia empresarial.

En este sentido, la colaboración con organizaciones empresariales y colectivos profesionales resulta indispensable, puesto que son estos los que trabajan directamente con el empresario.

2) Desplegar acciones de sensibilización basados en los beneficios del uso de servicios TIC y la seguridad proactiva.

Las Administraciones Públicas deben conocer las posibles reticencias de las empresas para utilizar servicios como la factura electrónica o la compra y venta online y trabajar para facilitar estos servicios e impulsar la e-confianza en la Sociedad de la Información.

En estrecha relación con lo anterior, es igualmente imprescindible desplegar acciones de difusión que combatan la falsa sensación de seguridad y promuevan la proactividad en la seguridad por parte de las empresas, con un enfoque basado en el riesgo.

Para ello, se deben habilitar canales informativos orientados a concienciar a los responsables de seguridad de las últimas novedades y riesgos, así como dar a conocer las soluciones que les puedan aportar, ya sea en forma de guías, indicadores, programas de formación o subvenciones estatales. Estos materiales informativos deben estar adaptados a las diferentes realidades que presentan las pequeñas y medianas empresas españolas.

3) Promover el desarrollo de estrategias empresariales basadas en estándares.

El apoyo de la Administración Pública se considera fundamental a la hora de generalizar la implantación de estándares, como los Sistemas de Gestión de la Seguridad la Información (SGSI).

Las empresas demandan, en este sentido, un mayor asesoramiento en el proceso de implantación y certificación, así como en el mantenimiento del mismo.

4) Desplegar acciones informativas y formativas para el personal de las empresas.

Extender la seguridad de la información al conjunto de la organización es una tarea que requiere realizar un esfuerzo que las pymes no siempre pueden acometer. Por ello, las Administraciones Públicas deben elaborar campañas informativas específicas y asesorar a las empresas en el diseño y realización de planes de formación específicos por perfiles de empleados.

5) Estudiar el estado de la seguridad de la información y la continuidad de negocio en las empresas españolas.

La realización de una labor recurrente de diagnóstico y métrica permitirá disponer de indicadores de la evolución en la implantación de herramientas y buenas prácticas de seguridad en las empresas y permite, a su vez, conocer el grado de efectividad de las diferentes acciones puestas en marcha por las Administraciones Públicas.

Con esta información, las empresas pueden comparar su posición respecto al resto del mercado. Por su parte, la industria de seguridad adecuará mejor su oferta a los diferentes perfiles de empresa. Por último, las AAPP podrán diseñar políticas públicas, orientar las acciones de divulgación y realizar un seguimiento del impacto de las mismas.

6) Realizar acciones específicas para las empresas de servicios de tecnologías de la información (TI).

Dado que muchas empresas de reducido tamaño confían los servicios TI en empresas externas subcontratadas, la Administración Pública debe incidir en que este colectivo adquiera un nivel adecuado de seguridad de la información y políticas de continuidad de negocio. Estas empresas externas pueden ejercer de palanca para que micro, pequeñas y medianas empresas consideren la seguridad de la información un requisito indispensable para el establecimiento de relaciones de negocio con otros proveedores y suministradores, así como una garantía de calidad con respecto a sus clientes.

ÍNDICE DE GRÁFICOS

Gráfico 1: Distribución de la masa laboral de empleados en España (%) 15

Gráfico 2: Distribución de las muestras por tamaño de la empresa (%) 17

Gráfico 3: Distribución del uso de tecnologías TIC (%) 24

Gráfico 4: Nivel de implantación declarado de soluciones de seguridad en la empresa (%) 26

Gráfico 5: Nivel de implantación declarado de las principales soluciones de seguridad Evolución 2009-2012 (%) 27

Gráfico 6 : Medidas de seguridad utilizadas/instaladas en los dispositivos móviles (%) 30

Gráfico 7: Percepción del nivel de seguridad de los dispositivos móviles frente equipos fijos y portátiles (%) 31

Gráfico 8: Servicios de red inalámbrica o wifi declarados por las empresas (%) 32

Gráfico 9 : Medidas de seguridad en redes wifi de la empresa (%) 33

Gráfico 10: Empresas que afirman contar con personas dedicadas a la seguridad de la información. Comparativa europea (%) 34

Gráfico 11: Disponibilidad de personal dedicado a la seguridad de la información (%) 35

Gráfico 12: Valoración del presupuesto en seguridad e informática en comparación con el año anterior (%) 36

Gráfico 13: Nivel de importancia que la dirección de la empresa otorga a la seguridad de la información (%) 37

Gráfico 14: Evolución percibida de la realización de copias de seguridad (%) 39

Gráfico 15: Evolución de la frecuencia declarada en la realización de copias de seguridad 2009-2012 (%) 40

Gráfico 16: Tipo de configuración declarada a la hora de realizar copias de seguridad (%) 41

Gráfico 17: Lugar donde las empresas almacenan las copias de seguridad (%) 42

Gráfico 18: Empresas que afirman aplicar restricciones en el acceso a *backups* (%) 42

Gráfico 19: Realización de actualizaciones del sistema operativo y programas (%) 43

Gráfico 20: Medidas de control de acceso a equipos y documentos (%) 44

Gráfico 21: Existencia de normas para la creación de contraseñas (%) 45

Gráfico 22: Disponibilidad de política de uso seguro de dispositivos móviles (smartphones, PDAs, tabletas, etc.) (%) 46

Gráfico 23: Existencia de límites de acceso a los servicios y contenidos de Internet para los empleados (%) 47

Gráfico 24: Percepción de la capacidad de los empleados para instalar programas (%) 48

Gráfico 25: Formación específica sobre riesgos de seguridad en las empresas (%)..... 49

Gráfico 26: Percepción de la realización de auditorías de seguridad en la empresa (%) 51

Gráfico 27: Empresas que declaran estar certificadas en ISO 27001 sobre Sistemas de Gestión de la Seguridad de la Información o SGSI (%) 52

Gráfico 28: Conocimiento de lo que es un Plan de Continuidad de Negocio (%) 53

Gráfico 29 : Evolución del grado de conocimiento “bueno” del PCN según tamaño (%) 54

Gráfico 30: Evolución de la previsión de alguna estrategia o procedimiento en caso de situaciones de crisis/desastre que afecten al negocio (%) 56

Gráfico 31: Razón por la que no se ha previsto una estrategia o procedimiento ante situaciones de crisis o desastre (%)..... 57

Gráfico 32: Posición afirmada por la empresa para afrontar una situación de crisis, desastre o contingencia (%)..... 58

Gráfico 33: Grado de identificación percibido de las operaciones críticas de negocio (%)..... 59

Gráfico 34: Evolución del tiempo máximo durante el que podría interrumpirse la actividad de la empresa sin suponer un impacto grave/crítico en el negocio (%) 60

Gráfico 35: Empresas que afirman disponer de un Plan de Continuidad de Negocio (%)..... 61

Gráfico 36: Conocimiento Vs. disposición en la empresa de un PCN, según sector de actividad (%) 62

Gráfico 37: Aspectos identificados dentro del PCN de la empresa (%)..... 63

Gráfico 38: Evolución de la disponibilidad de mecanismos para probar la eficacia del PCN en la empresa (%)..... 64

Gráfico 39: Empresas que afirman exigir a los proveedores algún nivel de servicio o un plan de gestión de la continuidad (%)..... 65

Gráfico 40: Evolución percibida en el último año sobre la seguridad en la empresa (%)..... 67

Gráfico 41: Empresas que afirman haber sufrido algún incidente de seguridad (%) 68

Gráfico 42: Incidentes vs. disposición de personal dedicado a seguridad (%) 68

Gráfico 43: Incidentes de seguridad reconocidos por las empresas (%) 69

Gráfico 44: Incidentes de seguridad declarados en los dispositivos móviles (%) 70

Gráfico 45: Tipología de incidentes declarados en los dispositivos móviles (%) 71

Gráfico 46: Incidentes de seguridad declarados que hayan impactado en la continuidad de los procesos u operaciones de negocio (%) 73

Gráfico 47: Tipología de incidentes de seguridad que han impactado en la continuidad de los procesos u operaciones de negocio (%) 74

Gráfico 48: Existencia de consecuencias derivadas de los principales incidentes de seguridad (%) 75

Gráfico 49: Reacción adoptada tras los incidentes de seguridad (%) 78

Gráfico 50: Resolución del incidente (%) 79

Gráfico 51: Resolución del incidente según el tipo de incidente vivido (%) 80

Gráfico 52: Utilización de servicios de Internet en la empresa. Comparativa europea (%) 81

Gráfico 53: Utilización declarada de servicios electrónicos a través de Internet por parte de las empresas (%) 82

Gráfico 54: Presencia de las empresas en las diferentes redes sociales (%) 84

Gráfico 55: Presencia de las empresas en las diferentes redes sociales, según tamaño (%) 84

Gráfico 56: Grado de confianza de las empresas en la utilización de la banca electrónica y los medios de pago online (%) 85

Gráfico 57: Grado de confianza de las empresas en las compras a través de Internet (%) 86

Gráfico 58: Grado de confianza de las empresas en la venta a través de Internet (%) 87

Gráfico 59: Grado de confianza de las empresas en la utilización de página web corporativa (%) 88

Gráfico 60: Grado de confianza de las empresas en la utilización de redes sociales (%) 89

Gráfico 61: Grado de confianza de las empresas en la utilización de redes sociales, en función de la red social utilizada (%) 90

Gráfico 62: Grado de confianza de las empresas en los trámites con la Administración (%) 91

Gráfico 63: Grado de confianza de las empresas en la firma electrónica (%) 92

Gráfico 64: Grado de confianza de las empresas en la factura electrónica (%) 93

Gráfico 65: Grado de confianza de las empresas en la contratación electrónica (%) 94

Gráfico 66: Distribución de empresas según sus perfiles de seguridad y e-confianza (%) 96

Gráfico 67: Distribución de las empresas en función de su perfil en materia de continuidad de negocio (%) 101

ÍNDICE DE TABLAS

Tabla 1: Universo del estudio 16

Tabla 2: Error muestral 19

Tabla 3: Disponibilidad de herramientas para proteger equipos y sistemas según tamaño de las empresas (%) 27

Tabla 4: Motivos señalados por las empresas para no utilizar las herramientas y soluciones de seguridad (%) 28

Tabla 5: Disponibilidad de personal dedicado a la seguridad según tamaño de empresa (%) 35

Tabla 6: Principales incidentes de seguridad declarados por las empresas según tamaño (%) 70

Tabla 7: Incidentes declarados en los dispositivos móviles según tamaño (%) 72

Tabla 8: Consecuencias derivadas de los principales incidentes de seguridad (%) 76

Tabla 9: Consecuencias que tuvo el incidente (%) 77

Tabla 10: Utilización de servicios electrónicos a través de Internet por parte de las empresas, según tamaño (%) 83

Tabla 11: Grado de confianza en la compra a través de Internet, según tamaño (%) 86

Tabla 12: Grado de confianza en la venta a través de Internet, según tamaño (%) 87

Tabla 13: Grado de confianza en la firma electrónica, según tamaño (%) 92

Tabla 14: Grado de confianza en la factura electrónica, según tamaño (%) 93

Tabla 15: Grado de confianza en la contratación electrónica, según tamaño (%) 94

Tabla 16: Motivos por los que las empresas no utilizan los servicios ofrecidos Internet (%) 95

Tabla 17: Perfiles de empresas sobre seguridad de la información y e-confianza 97

Tabla 18: Perfiles o grupos de empresas. Continuidad de negocio en la empresa 102

ANEXO I: BIBLIOGRAFÍA

- AETIC-EVERIS (2012). *Las tecnologías de la información y las Comunicaciones en la empresa española 2011* http://www.everis.com/spain/WCRepositoryFiles/Estudio_everis_AMETIC.pdf

- DELOITTE (2011) 2011 TMT *Global Security Study–Key Findings. Raising the Bar* http://www.deloitte.com/assets/Dcom-Croatia/Local%20Assets/Documents/2011/TMT_2011_Global_Security_Survey_hr.pdf

- DELOITTE (2010). *2010 TMT Global Security Study- Key findings. Bounce Back*. http://www.deloitte.com/assets/DcomGlobal/Local%20Assets/Documents/TMT/2010_TMT_Global_Security_study.pdf

- DGIPYME (2011) *Retrato de la Pyme en España*. http://www.ipyme.org/Publicaciones/Retrato_PYME_2011.pdf

- FUNDETEC (2011). *Análisis Sectorial de Implantación de las TIC en la PYME Española*. http://www.ipyme.org/Publicaciones/Informe_ePyme_2011_baja.pdf

- ICEX E-MARKET SERVICES SPAIN (2011) *El comercio electrónico en España – 2011*. http://www.emarketservices.es/icex/cma/contentTypes/common/records/mostrarDocumento/?doc=4528333

- INTECO (2010). *Estudio sobre el estado de la PYME española ante los riesgos y la implantación de Planes de Continuidad de Negocio*. http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_pymes_continuidad_negocio

- INTECO (2009). *Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas.* http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_seguridad_microempresas

- INTECO (2008). *Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*. http://www.inteco.es/Seguridad/Observatorio/Estudios/estudio_seg_pymes_2

- KASPERSKY LAB (2011). *Riesgos Globales a la Seguridad Informática*. http://www.df.cl/prontus_df/site/artic/20110902/asocfile/20110902172243/2_de_septiembre_informe_riesgos_globales_de_seguridad_de_ti.pdf

- NCIRCLE (2010). *2010 Information Security & Compliance Trend Study*. http://www.ncircle.com/pdf/studies/nCircle-WP-2010TrendStudy-1062-01.pdf

- ONTSI (2012). *Tecnologías de la Información y las Comunicaciones en PYMES y grandes empresas españolas*. http://www.ontsi.red.es/ontsi/sites/default/files/informe__pymes_y_grandes_empresas_2012-vf.pdf

- ONTSI (2012). *Tecnologías de la Información y las Comunicaciones en la microempresa española*. http://www.ontsi.red.es/ontsi/sites/default/files/informe__microempresas_2012-vf_0.pdf

- PANDA SECURITY (2011). *Informe Anual Pandalabs*. http://prensa.pandasecurity.com/wp-content/uploads/2012/01/Informe-Anual-PandaLabs-2011.pdf

- PANDA SECURITY (2010). *II Barómetro Internacional de Seguridad en las pymes*. http://prensa.pandasecurity.com/wp-content/uploads/2010/07/2ndbarometro.pdf

- PRICEWATERHOUSECOOPERS (2012) *Eye of de Storm. Key findings from the 2012 global state of information security survey*. http://www.pwc.com/es_CO/co/publicaciones/assets/global-state-of-information-security-survey-2011.pdf

- PRICEWATERHOUSECOOPERS (2009). *Trial by fire*. http://www.pwc.com/en_US/us/it-risk-security/assets/trial-by-fire.pdf

- RICHARD KISSEL (2009). *Small business information security: the fundamentals. National Institute of Standards and Technology*. http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

- SYMANTEC (2012). *Encuesta 2012 sobre Preparación ante Desastres en las PyMEs*. http://www.symantec.com/es/mx/theme.jsp?themeid=smb-disaster-recovery

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación